Rapport d'activité 2022






Sommaire



Le mot de la médiatrice



Marie-Christine Caffet
Médiatrice auprès
de la Fédération bancaire française (FBF)
depuis le 1er octobre 2018

PLUS DE 12 000 DEMANDES de médiation ont été reçues en 2022. La hausse de la recevabilité est importante : 45 % des saisines sont entrées tout de suite en analyse, certains groupes bancaires ou établissements atteignant désormais un taux de recevabilité dépassant 55 %. Cela est dû à la mise en œuvre progressive de la réforme de la procédure de réclamation issue des travaux du CCSF, mais aussi à l'amélioration des délais appliqués par les équipes chargées des réclamations dans les banques adhérentes.

Plusieurs établissements importants ont rejoint la médiation auprès de la FBF en 2022, expliquant la hausse des saisines. Près de 4 000 dossiers ont été traités en 2022.

Le flux élevé d'escroqueries a fait augmenter en proportion la part des propositions de solution partiellement favorables aux consommateurs, les banques ne pouvant être systématiquement conduites à la prise en charge des préjudices, dans la mesure où elles disposent désormais des moyens d'identifier avec précision les auteurs de la validation des opérations ou de fonder leur refus de remboursement sur une compromission de la confidentialité des données bancaires des consommateurs. En conséquence, les propositions de prise en charge partielle, ou de gestes en équité, ont été plus nombreuses.

Les autres raisons du recours à la médiation sont identiques à celles des années précédentes, avec toutefois la poursuite de la baisse des litiges portant sur la tarification et l'infléchissement très net des demandes de suspension des échéances de crédit.

L'utilisation des chèques continue de donner lieu à des détournements que quelques précautions d'usage (à recommander aux consommateurs) et quelques vérifications ou temporisations (à mettre en œuvre par les banques) pourraient contribuer à faire diminuer, qu'il s'agisse de chèques falsifiés, volés, ou encore de contrefaçons de chèques de banque lors de transactions entre particuliers.

Enfin, si les secousses supportées par les marchés financiers n'ont pas significativement augmenté les recours en médiation des épargnants, on continue de voir une progression significative des litiges portant sur des placements « miraculeux » ou en monnaie numérique qui ne procurent aux investisseurs que déception, ou se révèlent être des escroqueries. La hausse des taux d'intérêt devrait pouvoir ralentir l'appétit pour les livrets offrant des taux extravagants et replacer les supports à capital garanti en position plus attrayante.

Le rapport annuel de cette année 2022 est donc fortement concentré sur ces problèmes de fraudes. Mais il convient de ne pas oublier les autres sujets : ceux-ci font l'objet des cas illustrés par des collaborateurs de l'équipe de médiation, grâce auxquels près de 4000 dossiers ont été traités.

Il s'agit souvent de problèmes d'exécution des contrats et d'incompréhensions entre la banque et le consommateur, pour lesquels nous nous attachons à fournir toutes les explications nécessaires et proposons, quand c'est justifié, des solutions dont l'objectif est d'apaiser les relations. Comme je le soulignais l'année dernière, la Médiation bancaire ne peut se résumer à une rupture dans le parcours client, puisque la relation n'est pas rompue dans la très grande majorité des cas, le demandeur continuant d'utiliser quotidiennement les services de sa banque.

LORSQUE J'ÉCRIVAIS, IL Y A UN AN, que les litiges portés en médiation montraient la part grandissante des fraudes et des escroqueries reposant sur les opérations de paiement à distance, je ne pouvais prévoir que plus des trois quarts des dossiers traités en 2022 seraient consacrés aux suites à donner à ces méfaits.

La mise en place de l'authentification forte a été achevée au printemps 2021, elle permet désormais aux banques (prestataires de services de paiement, selon la terminologie en vigueur) d'identifier par deux facteurs, indépendants l'un de l'autre, qui est à l'origine de la validation de chaque opération.

Le dossier figurant dans ce rapport fait le point sur les nouveaux risques que ces process ont engendrés ou révélés :

- l'un des paradoxes auxquels les banques sont confrontées est d'avoir désormais les moyens de vérifier qu'un paiement a bien été autorisé par un client, mais pourtant celui-ci le conteste car il a fait l'objet d'une manipulation par un tiers, le poussant à consentir un acte à son détriment.

- L'autre paradoxe est que, malgré ces dispositifs, les fraudes se développent en profitant des conséquence de la multiplication des acteurs présents sur toute la chaine des paiements : censées favoriser la concurrence au bénéfice du consommateur, ces multiples solutions de paiement se superposent et sont difficilement comprises par certains de leurs utilisateurs; nombre de ces derniers, croyant notamment faciliter leurs opérations entre particuliers, renseignent malheureusement leurs données bancaires sur des sites malveillants, qui imitent parfaitement ceux d'acteurs connus ou ceux de nouveaux prestataires, ouvrant ainsi l'accès à leurs comptes en ligne.

La jurisprudence actuelle n'a pas encore tranché sur ces points majeurs, pour déterminer la responsabilité du payeur et de la banque du payeur, **mais aussi celle des intermédiaires** – agrégateurs (PSIC), établissements de paiement, prestataires de services d'initiation de paiement (PSIP)… en cas de contestation. D'un côté, on voit le reproche de négligence grave être invoqué dans chaque refus de remboursement, sans distinguer ce qui relève du consentement de ce qui est la résultante d'une imprudence. De l'autre, on voit se multiplier les réclamations s'appuyant sur la revendication d'un droit systématique au remboursement de toute opération contestée, sans que soient distingués d'une part les paiements connus et validés par le titulaire du compte et d'autre part les paiements réellement faits à l'insu du titulaire du compte.

Par ailleurs, la réglementation européenne applicable aux paiements a rendu plus complexe, pour les consommateurs comme pour les banques, la détection des opérations suspectes : elle repose en effet sur la dissociation de l'initiation du paiement (qui peut émaner d'un prestataire spécialisé, d'un établissement de paiement… mais aussi d'un fraudeur) de la forme de sa validation par le payeur.

En séparant l'initiation des paiements de leur validation, l'authentification forte permet en principe aux titulaires d'instruments de paiement et de comptes bancaires d'avoir la maitrise de leurs transactions, quels que soient l'initiateur et le lieu de l'opération, et d'écarter toute utilisation à leur insu, puisque leur consentement ne peut avoir été recueilli que sur leur dispositif personnel, installé sur leur appareil personnel; dans une forme plus simple, le consentement peut également reposer sur deux codes indépendants, dont le principal est créé par le payeur et ne circule pas par messagerie.

Mais le détricotage de la chaine des paiements a aussi ouvert aux escrocs en tout genre de multiples portes par lesquelles ils peuvent se faufiler en profitant des allègements de procédures exigés par les nouveaux acteurs qui souhaitent s'installer sur ce marché des paiements : le dum-

ping des sécurités se masque alors derrière la nécessité de lever des barrières à l'ouverture à la concurrence, voire derrière une prétendue «fluidité du parcours client» qui exigerait que tout paiement soit fait en deux clics et instantanément etc. Ainsi, l'enrôlement «à la volée» des cartes bancaires sur les portefeuilles électroniques a donné lieu en 2022 à de très nombreux détournements, facilités par la simple implémentation d'un code à usage unique pour utiliser n'importe quelle carte, lequel code étant intercepté sans grande difficulté par des fraudeurs, voire par des proches.

Au terme d'une conférence de mars 2022 de France Payment forum portant sur l'Europe des services bancaires et financiers, les principaux intervenants insistaient sur la nécessité de «*contraindre les grands acteurs internationaux à respecter les principes de concurrence en Europe et au rejet de leurs pratiques discriminatoires*». Toutes les directives européennes vont dans le même sens : permettre l'émergence d'acteurs offrant des services moins onéreux, plus agiles et qui peuvent accéder aux données des clientèles de la banque de détail, qui sont leur cible de conquête.

Nous y sommes, mais force est de reconnaitre que **la sécurité de l'accès aux données** ainsi que la protection des avoirs des clientèles concernées ouvrent un chantier largement inentamé, en tout cas sous exploité, vraisemblablement parce qu'il a été mal évalué. Ce que l'on appelle parfois le «facteur humain» est au cœur du sujet : comment peut-on sérieusement considérer qu'un consommateur est toujours à même de choisir de façon rationnelle le meilleur service ou produit, comment protéger au mieux ses données et ses fonds, étant donné la **complexité** grandissante de ces process et de ces produits? À titre d'illustration, les trois quarts des utilisateurs de dispositifs d'authentification forte reposant sur une application bancaire installée sur leur téléphone ne savent même pas que les notifications de paiement qui arrivent sur leur écran ne transitent pas par leur ligne téléphonique et que ce ne sont pas des SMS…

Les mots «*pratiques discriminatoires*», utilisés parfois de façon indifférenciée pour s'attaquer aux pratiques restrictives que pourraient rencontrer des concurrents, ne peuvent viser les précautions consistant à faire obstacle aux connexions émanant d'escrocs et de fraudeurs; les considérations et recommandations en faveur de l'ouverture de l'accès aux données révèlent aussi la pression des nouveaux acteurs sans que de leur côté les consommateurs soient suffisamment protégés. Or, les conditions de cet accès sont à la main des régulateurs*[1].

Il est grand temps que les associations de consommateurs fassent de ce chantier de la sécurité un enjeu majeur de leurs propositions, car faire rembourser les banques dans n'importe quelle circonstance ne peut qu'encourager les fraudeurs à multiplier leurs méfaits.

Du côté des banques, il est aussi grand temps que l'authentification forte soit requise lors de chaque connexion nouvelle à l'espace bancaire de leurs clients, pour repérer les tentatives d'intrusion dans leur compte en ligne : **plus de la moitié des fraudes actuelles sont accompagnées ou précédées de ces connexions inhabituelles.**

Je rappelle que le but des «parcours digitaux» n'est pas de restreindre les relations de proximité entre les banques et leurs clients, en leur laissant la charge de faire eux-mêmes tous les paiements, mais de faire bénéficier tous ceux-ci de l'exécution rapide de leurs opérations, dans une grande sécurité. ◆

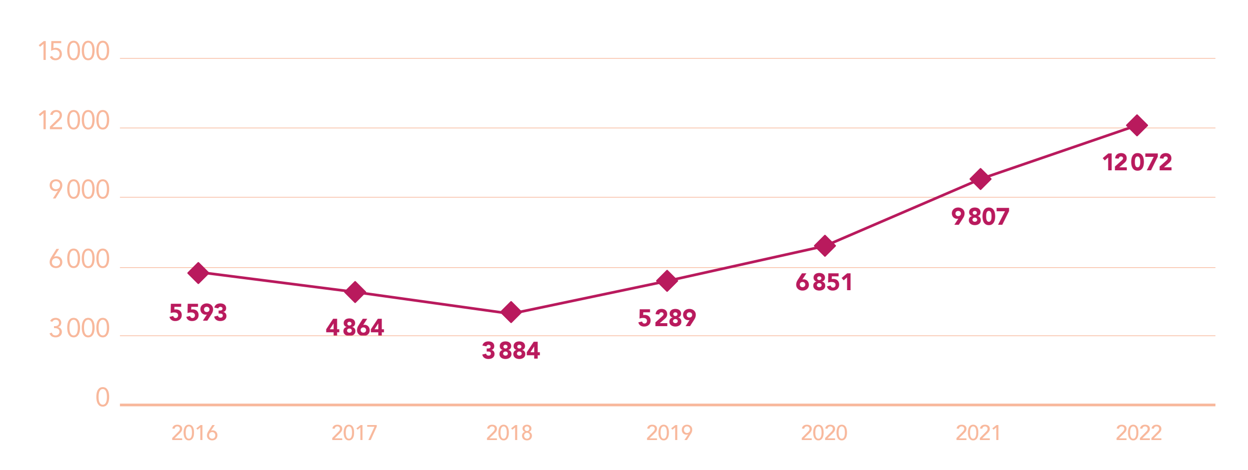
* Puisque le règlement «P2B» ne régule pas l'accès aux données en lui-même mais prévoit simplement que les conditions générales doivent comprendre une description de l'accès, ou de l'absence d'accès, des utilisateurs professionnels à toutes données personnelles ou autres données, ou les deux., cf la loi n° 2020-1508 du 3 décembre 2020 portant diverses dispositions d'adaptation au droit de l'Union européenne en matière économique et financière dite loi «DDADUE», qui prévoit le rattachement du règlement «P2B» au droit national prohibant les pratiques restrictives de concurrence.

Les chiffres de l'année 2022

Les demandes de médiation reçues en 2022

Une hausse de 23 % du nombre de dossiers reçus en 2022 par rapport à 2021.

12 072 demandes de médiation ont été formulées par les consommateurs.



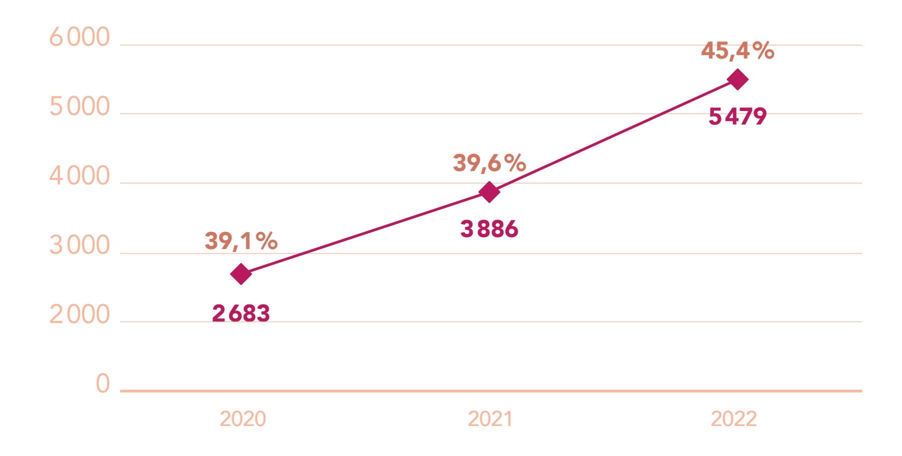
Cette augmentation régulière depuis 2020 est liée :

- à l'accueil de nouveaux adhérents,
- à l'augmentation sensible, cette année encore, des litiges portant sur des escroqueries.

40 % des demandes de médiation arrivent par courrier.

Le traitement des demandes de médiation en 2022

Sur ces 12 072 demandes, 9 807 respectent les critères posés par la loi et relèvent de la compétence de la Médiatrice.
Les dossiers immédiatement recevables, respectant les conditions posées par la Loi (passage préalable par une réclamation, qu'elle soit ou non satisfaite), sont en nette progression.



Sur les 12072 dossiers reçus en 2022, 45 % ont été déclarés recevables par la médiatrice.

Ce chiffre, en progression, est le résultat du début d'application des recommandations des autorités de supervision : pour l'application des critères de recevabilité édictés à l'article L 612-2 du code de la consommation, la preuve de la réclamation écrite faite au professionnel est valable quel que soit le service auquel elle a été adressée.

6593 demandes de médiation n'ont pas pu être traitées, ventilées de la façon suivante :

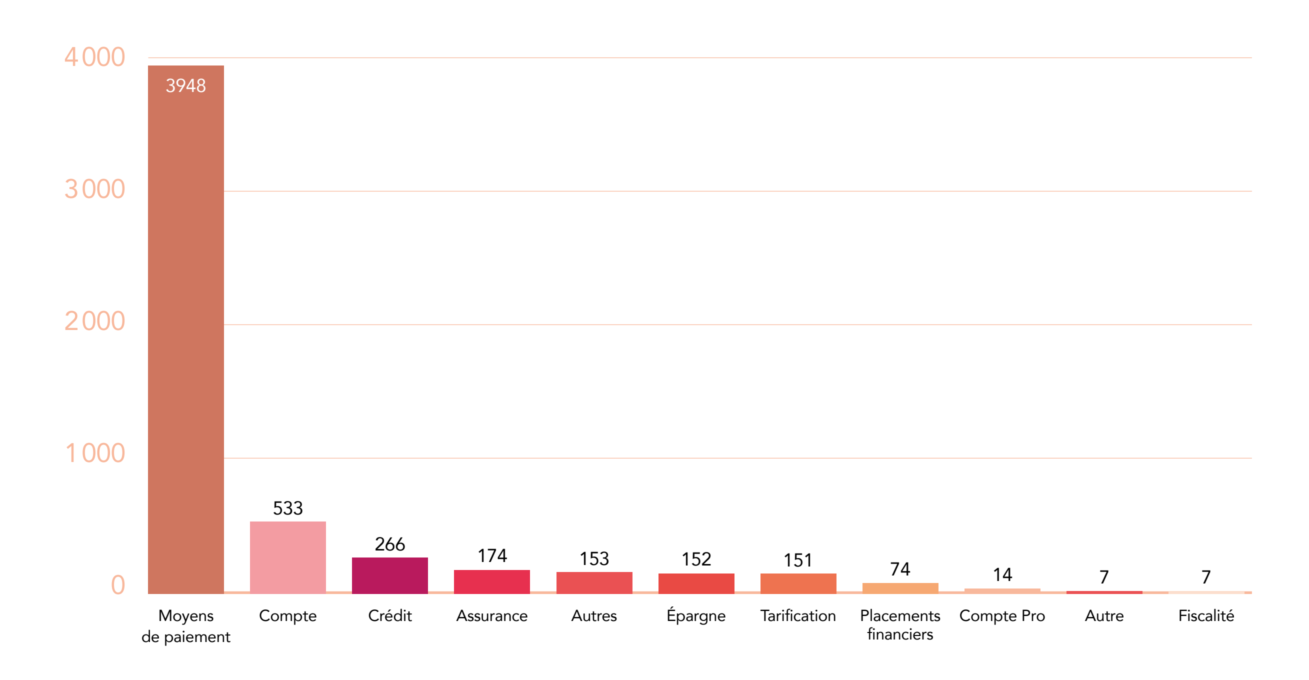
- **5106 saisines précoces** (sans réclamation préalable)
- **59 saisines postérieures** à la saisine d'un tribunal
- **51 demandes hors du champ de compétence** de la médiatrice
- **38 saisines** adressées alors que la réclamation date de plus d'un an
- **29 dossiers non éligibles**
- **3 saisines abusives** ou infondées

Par ailleurs, nous avons comptabilisé **36 retraits du processus de médiation** et **19 refus d'entrer en médiation** du professionnel. Ces refus ont majoritairement concerné un établissement, mais également quelques banques traditionnelles et une banque en ligne.

Enfin, les principales explications du solde des demandes non traitées sont :

- dossiers réorientés vers le bon médiateur, choisi par le professionnel (549),
- absence ou insuffisances d'information (341),
- dossiers envoyés en doublons (310) et dossiers incomplets.

Les sujets de mécontentement des consommateurs



Avec toujours une nette prévalence des escroqueries.

Les enjeux financiers

- Montants des préjudices estimés par les consommateurs

Nombre de dossiers :

Estimation financière requête	2020	2021	2022
< à 500€	477	609	666
de 500 à 1000€	408	557	795
de 1000 à 5000€	705	1200	1987
de 5000 à 10000€	117	236	563
> de 10000€	197	270	440
Sans estimation financière	131	161	184
Inconnu	648	853	844
Total	**2683**	**3886**	**5479**

- Montants proposés par la Médiatrice

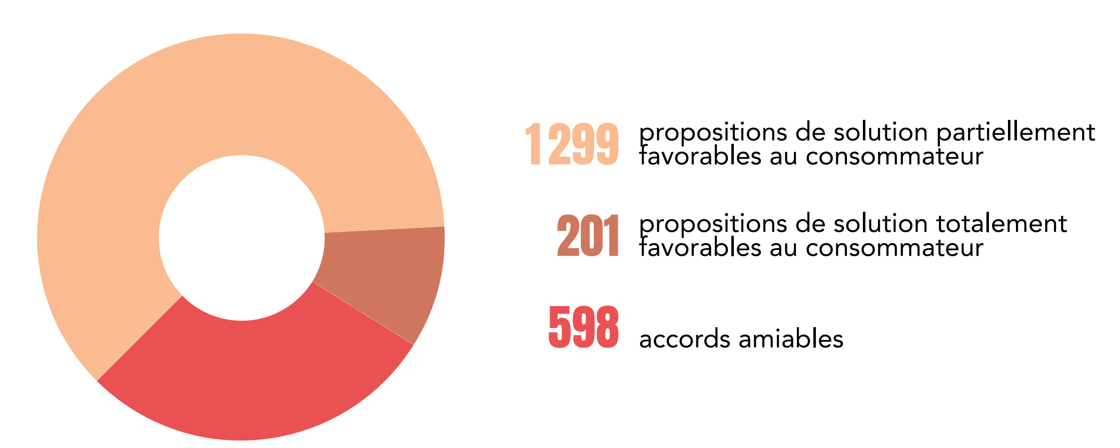
Montant(s) proposé(s)	Nombre de dossiers	Moyenne des montants accordés
< à 500€	**892**	**175,94**
de 500 à 1 000€	**248**	**681,71**
de 1 000 à 5 000€	**305**	**1 956,64**
de 5 000 à 10 000€	**32**	**6 296,26**
> de 10 000€	**23**	**61 030,575**

3 915 litiges ont été résolus en 2022 grâce à l'action de la Médiatrice

3 317 propositions de solution ont été adressées aux parties et **598 règlements amiables** ont été conclus entre les parties.

2 098 différends ont été résolus en faveur du consommateur et 1817 en faveur de la banque.

Le chiffre de 2 098 dossiers favorables au consommateur se décompose en :



Comment les parties ont-elles accueilli les solutions qui leur étaient partiellement ou totalement favorables ?

Les banques ont accepté de répondre positivement aux demandes faites par le consommateur et la Médiatrice dans 74,5 % des cas.

Lorsque la solution était totalement ou partiellement favorable, les consommateurs ont accepté la solution dans 80 % des cas.

Les délais de traitement

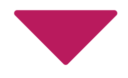
Cette année, nous déplorons des délais plus longs que les autres années. Ceci est dû à 3 facteurs :

- **l'augmentation du nombre de demandes** de médiation
- **l'arrivée de nouveaux établissements adhérents** au service de médiation
- **des collaborateurs en arrêt** de longue durée

Le délai moyen de traitement d'un dossier à compter de la réception des éléments de la banque est de 101 jours et de 130 à compter de la notification de la recevabilité aux parties.

Focus

RENFORCER LA SÉCURITÉ DES PAIEMENTS EN LIGNE : LES DÉFIS DE L'AUTHENTIFICATION FORTE



Les premières données disponibles de l'Observatoire de la sécurité des paiements concernant 2022 montrent que le **taux de fraude** continue de baisser de façon significative.

Pourtant, et c'est un paradoxe apparent, les victimes de détournements sont aujourd'hui moins souvent éligibles à une prise en charge de leur préjudice par la banque : en effet, depuis le déploiement de l'authentification forte, celle-ci peut désormais avoir la preuve que le paiement a été validé par leurs soins ou, à l'inverse, que l'opération a été validée par un fraudeur, à la suite de la compromission de leurs données de sécurité personnalisées.

Il convient donc en premier lieu de distinguer ce qui est une opération *autorisée* et ce qui est une opération *non autorisée*, en rappelant que la seule contestation d'un paiement par le titulaire d'un compte ne suffit pas à qualifier l'opération, du point de vue de la réglementation bancaire.

Il conviendra ensuite, en considération des nouvelles formes que prennent les fraudes et les escroqueries, d'examiner comment y faire obstacle.

Le caractère autorisé ou pas d'une opération résulte de la procédure suivie en matière de consentement et de la connaissance qu'en avait le payeur.

Pour qu'un paiement soit « non autorisé », il faut :

- que le payeur n'ait pas autorisé l'opération selon les formes requises par la réglementation, et donc qu'il ne l'ait pas validée **lui-même** en authentification forte pour un paiement par carte ou un virement à distance ;

- **et** que ce paiement ait été ordonné et validé **à son insu**, sans qu'il en ait eu **connaissance**.

À ce stade, rappelons que la forme du consentement n'est pas précisée dans le code civil mais qu'en revanche, pour les paiements régis par le code monétaire et financier, elle renvoie aux conditions générales convenues entre les parties, lesquelles sont alors d'interprétation stricte (notamment les articles L 133-6 et 133-44).

Rappelons aussi que l'authentification forte repose sur l'utilisation de deux éléments ou plus appartenant à deux catégories différentes de facteurs, parmi les trois suivantes :

- « connaissance » : une information que seul l'utilisateur connaît, par exemple un code confidentiel, un mot de passe ou une information personnelle ;

- « possession » : un objet, un appareil ou un service que seul l'utilisateur possède, et qui peut être reconnu sans risque d'erreur par la banque, comme un smartphone, une montre ou un bracelet connecté, etc. , mais aussi une messagerie téléphonique personnelle ;

- « inhérence » : un facteur d'authentification propre à l'utilisateur lui-même, c'est-à-dire une caractéristique biométrique (empreinte digitale, visage, voix…).

La Directive européenne dite DSP2 dispose que ces éléments doivent être indépendants : la compromission de l'un ne doit pas remettre en question la fiabilité des autres facteurs, de manière à préserver la confidentialité des données d'authentification.

On voit deux procédures d'authentification forte

Aujourd'hui, en France, deux procédures d'authentification forte sont proposées aux clients des banques :

- Un dispositif reposant sur une **application bancaire**, enrôlée sur un appareil personnel (terminal de confiance) qui est enregistré par la Banque. La validation des opérations se fait en apposant son empreinte biométrique sur l'application, ou par saisie de son code personnel sur cette application ; quel que soit le terminal où a été initié un paiement, c'est le détenteur de l'appareil où est installée l'application qui devra autoriser ou refuser lui-même l'opération.

- Un dispositif alternatif reposant sur **deux codes**, lequel s'adresse généralement aux clients désireux de ne pas utiliser leur téléphone mobile (smartphone ou équivalent). La validation des opérations se fait en saisissant successivement les deux codes, sur une fenêtre s'ouvrant à partir du site marchand ou du terminal où a été initié le paiement ; l'un de ces codes est strictement personnel et confidentiel, connu du seul client (il ne circule pas par messagerie), l'autre est envoyé généralement par SMS sur la messagerie personnelle du client.

Une exigence de réitération systématique

Les données d'authentification doivent être liées à l'opération de paiement, de sorte qu'elles ne peuvent être réutilisées pour une opération de paiement ultérieure :

- ainsi, le code d'authentification (ou l'utilisation du facteur biométrique) appliqué pour l'opération est spécifique au montant de l'opération et au bénéficiaire identifié ;

- en outre, toute modification du montant ou du bénéficiaire nécessite une nouvelle authentification.

(source les travaux de l'OSMP avril 2023)

Une envolée des escroqueries par vishing

La question de la confirmation du caractère autorisé d'une opération se pose en des termes différents depuis que de nombreuses escroqueries se sont développées, consistant à amener un payeur, généralement par tromperie au cours d'un échange téléphonique, à valider **lui-même**, sur son appareil personnel, des opérations initiées par un fraudeur, croyant que celui-ci (qui prétend être sa banque) va les annuler ou les rembourser ; dans le système reposant sur deux codes, lesdits codes sont sollicités ou obtenus par le fraudeur (qui les saisira sur son propre terminal) au moyen d'un hameçonnage similaire.

Je rappelle immédiatement que l'escroquerie constitue un délit qui relève de la justice pénale et que les banques sont concernées **uniquement**, en pareil cas, par l'exécution des opérations de paiement contestées, pour lesquelles elles doivent prouver la sécurité de leurs procédures et la clarté du recueil du consentement de leurs clients.

Force est aussi de constater que de nombreux consommateurs, quand ils en sont victimes, vont déposer plainte auprès de la Police ou de la Gendarmerie et sont alors renvoyés vers leur établissement avec d'une part une note d'information listant quelques articles du code monétaire et financier sans en expliquer les modalités d'application et, d'autre part, l'indication qu'ils doivent être remboursés par leur banque quel que soit leur rôle dans le déroulement de l'escroquerie.

Ces deux préalables étant rappelés, la sophistication des manipulations amène toutefois, pour les dossiers arrivant en Médiation, à tenir compte des circonstances pour apprécier les responsabilités respectives de la banque et du consommateur.

En effet, de nombreux clients victimes de ces agissements réfutent avoir consenti à faire ces paiements en mettant en avant trois arguments :

- ils ne les ont pas *initiés*; en effet, c'est le fraudeur, dans les cas de paiements par carte bancaire, qui a renseigné les données de la carte sur les sites commerçants; pour les virements, c'est le fraudeur, après s'être introduit dans l'espace bancaire du client, qui a saisi les données d'un IBAN frauduleux;

- leur consentement aurait été *vicié*;

- ils ont été soumis à une pression qui aurait *altéré* leur consentement.

- Sur l'initiation des paiements à partir de l'appareil de l'escroc, il faut souligner que la distinction entre initiation et validation d'une opération est une conséquence des textes européens et qu'elle ne peut permettre de mettre en cause, à elle seule, le caractère autorisé d'un paiement. Une illustration très simple est que beaucoup d'internautes saisissent sur leur ordinateur personnel les données de leur instrument de paiement pour acheter un bien ou un service et valident sur un autre appareil (leur smartphone) l'opération, ce qui distingue bien l'initiation de la validation. En revanche, toujours sur ce point, il faut savoir que de plus en plus de juridictions considèrent qu'est nécessairement fautif celui qui donne son accord à une opération dont il n'est pas à l'origine. En résumé, l'initiation de paiements à partir d'appareils ou adresses IP différentes de celle de l'utilisateur de l'appareil de validation (enregistré par la banque) peut effectivement permettre de détecter une ou des opérations suspectes, elle n'en détermine cependant pas, avant comme après, le caractère autorisé.

- Sur le vice du consentement, les dispositions du Code civil (dol ou erreur) ne paraissent pas pouvoir être invoquées : le dol doit émaner du cocontractant, or ce n'est évidemment pas leur banque qui est à l'origine de la tromperie. Quant à l'erreur, au sens du Code civil[1], il faut qu'elle porte sur la qualité essentielle de la prestation ou du contrat; or, le seul contrat existant est celui entre la banque et son client, il porte sur le recueil de l'autorisation de paiement et les obligations de chacune des parties lors de la réception d'un ordre de paiement par la Banque :

  - d'une part l'obligation du payeur, qui doit utiliser ses données de sécurité personnalisées et son dispositif d'authentification pour valider tout paiement qu'il a lui-même décidé, **ou le refuser dès lors qu'il n'en n'est pas à l'origine;**
  - d'autre part l'obligation de la banque, qui se doit de l'exécuter dès qu'il a été validé selon les formes et les modalités requises, ou le bloquer s'il a été refusé.

L'erreur, si elle devait être retenue, porterait en réalité non sur un consentement involontaire aux paiements mais sur l'absence d'annulation ultérieure des opérations, par le fraudeur!

En résumé, l'invalidation de l'authentification pour réfuter le consentement d'un payeur ne pourrait s'appliquer que si l'un des deux co-contractants – ici la Banque – avait induit en erreur l'autre partie, d'une façon ou d'une autre (notification confuse, absence d'identification de la part de la Banque, erreur de saisie ou d'exécution etc.).

1. Article 1123 du Code civil : L'erreur de droit ou de fait, à moins qu'elle ne soit inexcusable, est une cause de nullité du contrat lorsqu'elle porte sur les qualités essentielles de la prestation due ou sur celles du cocontractant.

- Sur l'altération du consentement : lorsque l'escroquerie a pris la forme d'un spoofing (usurpation crédible de la qualité de la banque en affichant son identité téléphonique), la victime, de toute bonne foi, a obéi aux instructions de son interlocuteur qui lui enjoignait de valider un ou plusieurs paiements, en pensant qu'il allait les annuler. Pour en apprécier l'étendue et la réalité, et déterminer si les paiements ont été valablement consentis, il convient d'examiner plusieurs points :

  > le contenu des notifications visant à authentifier les paiements et ensuite des notifications de confirmation des opérations, après chaque achat ou chaque virement ;

  > la connaissance qu'avait l'utilisateur des fonctionnalités de son dispositif : un consommateur qui ne fait jamais ou rarement de paiements à distance ou qui vient d'équiper son appareil n'est pas dans la même situation qu'un payeur familier de ces outils ;

  > le nombre d'opérations validées : si la première opération peut effectivement résulter d'une confusion ayant altéré la valeur du consentement, sous la pression, une simple lecture des messages de confirmation pouvait suffisamment éclairer l'utilisateur pour qu'il stoppe ensuite ses validations ;

  > l'existence de SMS frauduleux, parallèles et concomitants aux notifications, venant chevaucher ces dernières pour prétendre avoir annulé les paiements après chaque validation ; l'altération du consentement est alors manifeste et doit être prise en considération par la Banque, la Médiation proposant une prise en charge conséquente et en fonction du déroulement des faits.

Dans les cas avérés de spoofing (avec affichage du nom, du numéro de la banque voire du conseiller), le client qui en est victime est forcément ébranlé et ne peut raisonnablement comprendre ce qui lui arrive, au moins dans les premiers échanges avec son interlocuteur malveillant. Ensuite, ce sont les injonctions reçues qu'il faut examiner, pour déterminer s'il s'agit de demandes crédibles ou extravagantes (certains escrocs demandent à leurs victimes d'autoriser des virements sur un compte externe pour « mettre à l'abri » leurs fonds, ou leur envoient un coursier pour récupérer la carte bancaire et le code).

En synthèse, quelle que soit la conclusion sur la qualification de l'opération contestée, et même si la Banque peut prouver que le valideur est le payeur, il faut encore apprécier les circonstances de chaque opération.

- Lorsque l'authentification forte a été appliquée sous la forme de deux codes : dans cette procédure, souvent appelée « SMS renforcé », la banque ne peut évidemment pas déceler si la validation a été faite par les soins du payeur ou (ce qui est le cas général) par le fraudeur qui s'est fait communiquer les codes ; en effet, l'initiation et la validation de l'opération sont saisies à partir de l'adresse IP du fraudeur, que ne peut connaitre la banque. Il s'agit alors et sans aucun doute d'une opération non autorisée : le paiement a été validé à l'insu du titulaire du compte puisqu'il n'a pas saisi lui-même les deux codes. Il incombe donc à la Banque, si elle refuse le remboursement, de prouver la négligence grave et d'appliquer, en attendant, l'article L 133-18 du code monétaire et financier pour éviter d'éventuels dépassements de découvert ou frais d'incident.

La recrudescence des escroqueries et tout particulièrement des cas d'intrusion dans les espaces de banque en ligne doit amener au renforcement des obligations d'authentification forte

La connexion des fraudeurs aux espaces bancaires des clients victimes de détournements représente désormais plus de la moitié des cas de contestations d'opérations venant en Médiation.

La loi impose l'authentification forte

L'article L.133-44 du code monétaire et financier **prévoit que l'authentification forte est requise** «*lorsque le payeur (…) Accède à son compte de paiement en ligne*». L'authentification forte lors de chaque connexion à l'espace bancaire est donc imposée par la Loi.

L'exemption accordée aux prestataires de services de paiement et à tous les acteurs de la chaine des paiements consiste à ne la demander que périodiquement (tous les 90 jours et bientôt tous les 180 jours), et ne s'applique que lorsque l'accès est limité aux consultations du solde et des mouvements antérieurs, ce qui résulte d'un règlement délégué de la Commission européenne (UE 2018/39).

L'absence d'authentification forte lors de la connexion au compte est à l'origine des principales escroqueries

Le défaut d'authentification forte est à l'origine de la majorité des cas d'escroquerie qui sont arrivés en Médiation : les fraudeurs ont en effet 89 jours et bientôt 179 jours pour s'introduire dans les comptes en ligne sans que leurs titulaires puissent les y autoriser explicitement.

La connexion frauduleuse résulte généralement d'une interception des données personnelles du titulaire d'un compte à la suite de la saisie malencontreuse de ses identifiants et du code d'accès sur **un site miroir d'un établissement de paiement**, laquelle contrefaçon est parfaitement indécelable, tandis que s'interrompt la session dès que les renseignements utiles ont été obtenus. Le titulaire, de toute bonne foi, réitère souvent ses tentatives, parfois sur le bon site.

Une fois récupérés les codes d'accès, le fraudeur se connecte et peut alors connaître toutes les informations sur le solde et les dernières opérations exécutées, afin qu'il s'en serve lors d'un «vishing» pour persuader sa victime qu'il échange avec son conseiller. Cela lui permet également de procéder à des virements internes, ces derniers étant également exonérés d'authentification forte par le règlement délégué susvisé, dès lors que le payeur et le bénéficiaire sont une seule et même personne et que les comptes sont détenus dans le même établissement.

Il peut aussi avoir saisi les données d'IBAN de comptes externes avant de faire valider leur enregistrement par sa victime, en insistant par pression lors d'un appel téléphonique, le malheureux titulaire ne pouvant déceler sur le moment que les chiffres saisis ne concernent pas ses bénéficiaires (il arrive même que le fraudeur ait libellé l'IBAN au nom du titulaire légitime du compte).

Ainsi les fraudeurs, lorsqu'ils sont «dans la place» sans que le titulaire du compte ait pu le détecter, ont les moyens de commencer à préparer leurs méfaits.

Si la responsabilité personnelle du titulaire du compte reste engagée en cas d'intrusion frauduleuse, en pareil cas le défaut d'authentification forte au moment de la connexion engage aussi et subsidiairement la responsabilité de la Banque.

Les travaux récents de **l'Observatoire de la sécurité des moyens** de paiement ont heureusement abouti à une recommandation de requérir systématiquement l'authentification forte lorsque la connexion se fait par un **appareil inhabituel.**

Mais cette recommandation doit aussi être replacée dans son contexte : elle s'inscrit dans un paysage européen largement encadré par des dispositions allant dans le sens contraire

Le règlement délégué déjà cité vient de connaitre une modification qui instaure de facto une sorte «d'exemption obligatoire» à compter de juillet 2023, que la Commission considère nécessaire puisque l'authentification systématique serait un obstacle à la consultation des comptes par les agrégateurs (dans le jargon européen, il s'agit des PSIC prestataires de services d'information sur les comptes).

Or, le considérant 6 du règlement UE 2022/2360 opère une distinction selon qu'il s'agit des teneurs de compte (les banques), qui «*sont autorisés à ne pas appliquer*» l'authentification systématique à chaque connexion, ou qu'il qu'il s'agit d'intermédiaires (PSIC en l'espèce, mais il est évident que les initiateurs dénommés PISP seront également visés) qui «*n'appliquent pas l'authentification forte*» lorsque l'accès consiste en une simple consultation. En somme, il y a des autorisations facultatives et des exemptions obligatoires.

Le point 3 de l'article 10 bis prévoit toutefois que les banques sont autorisées à appliquer l'authentification forte lors d'une connexion passant par l'intermédiaire d'un agrégateur (PSIC), en cas de soupçon de fraude; mais elles doivent justifier ces demandes auprès de leurs régulateurs.

Ainsi, la multiplication des acteurs intervenant dans la chaine des paiements va désormais ouvrir de nombreuses voies d'accès aux comptes, en facilitant «le parcours client» (en réalité celui des établissements intermédiaires, au nom de la concurrence); mais ces facilités seront inévitablement exploitées par les escrocs, si des mesures de sécurité ne sont pas mises en œuvre. Or, elles sont combattues par les nouveaux acteurs et, manifestement, la voix des associations de consommateurs ne porte généralement pas sur ce point, ou, lorsqu'elles s'emparent du sujet, n'est pas audible ou même entendue.

Les voies et conséquences des intrusions

Parmi les failles d'authentification exploitées par les escrocs, on recense désormais :

- la saisie des données du compte bancaire sur l'interface apparente d'autres établissements de paiement, le titulaire légitime ne faisant pas la différence entre saisir les chiffres de son IBAN et ceux de l'identifiant et de son code d'accès;
- le piratage de plusieurs comptes internes résultant de l'accès par un intermédiaire agrégateur;
- l'enrôlement au dispositif d'authentification forte de la banque et/ ou son transfert sur le terminal du fraudeur, sans que le titulaire ait pu remarquer l'intrusion préalable;
- les modifications de paramètres et de plafonds de paiements après que le dispositif a été détourné;
- les virements internes et ensuite au profit de comptes ouverts dans d'autres banques, sans authentification forte grâce à l'agrégation;
- l'émission de virements vers des bénéficiaires dont les IBAN ont été créés ou modifiés par le fraudeur mais validés par le titulaire;
- quelques premiers cas résultant d'une API («application programming interface») qui permet de «connecter» un logiciel ou un service à un autre logiciel ou service afin d'échanger des données et des fonctionnalités. L'API, dédiée à l'initiation de paiement par virement, permet d'effectuer des virements depuis le site de «e commerçants» qui fournissent ainsi une nouvelle option de paiement; or, ce type d'opération implique la nécessité préalable pour le client de **saisir depuis le site du commerçant ses données de sécurité personnalisées** lui permettant de se connecter sur son espace en ligne bancaire pour initier le virement. Même si l'opération est ensuite authentifiée fortement, les données d'accès à son compte ont pu être renseignées sur une interface que les fraudeurs ont alors consultée.

En conclusion, je souligne à nouveau la nécessité de combattre toute forme de dumping de sécurité et du côté des banques, d'accroitre leurs moyens de surveillance des connexions et des opérations passant par ces nouveaux canaux.

Le chantier de l'OPEN FINANCE, qui s'ouvre à Bruxelles, a rendu ce sujet stratégique : après avoir concerné les moyens de paiement des consommateurs, la consultation par des acteurs tiers de l'ensemble de leurs données (produits d'épargne, crédits), sera autorisée notamment via des interfaces dont la sécurité devra évidemment être une priorité. ◆

Cas pratiques

▸ Paiements frauduleux non authentifiés et déclarés tardivement à sa banque



Morgane

Les faits

Monsieur X souhaite obtenir le remboursement de 325 opérations de paiement à distance par carte bancaire effectuées entre septembre 2020 et août 2021. Il précise qu'il est toujours en possession de sa carte, qu'il ne l'utilise jamais pour effectuer des paiements sur internet et qu'il n'a répondu à aucun courriel ou SMS frauduleux.

La Banque indique que les paiements frauduleux n'ont pas été authentifiés. Toutefois, elle souligne que la contestation de Monsieur X, reçue début août 2021, est très tardive. La Banque lui a donc proposé un remboursement partiel à hauteur de 30 % des opérations litigieuses, ce que Monsieur X a refusé.

Monsieur X demande donc le remboursement des 325 paiements litigieux.

L'analyse de la Médiatrice

Ne disposant d'aucun élément me permettant de comprendre les circonstances des opérations litigieuses, je relève qu'il m'est difficile d'apprécier et de déterminer une éventuelle défaillance de la part de Monsieur X dans le respect de ses obligations de conservation de ses données de sécurité personnalisées issues de l'article L.133-16 du Code monétaire et financier.

Je constate ensuite que le montant de chaque paiement frauduleux est très peu élevé, ce qui me parait révéler des utilisations discrètes pouvant suggérer une « fraude relationnelle ». J'invite donc Monsieur X à protéger sa carte de

toute utilisation par son entourage et à la ranger dans un lieu empêchant toute consultation.

Par ailleurs, j'observe qu'au sens de l'article L.133-23 du code susmentionné, la Banque n'est pas en mesure de prouver que les opérations litigieuses ont été authentifiées, dûment enregistrées et comptabilisées et qu'elles n'ont pas été affectées par une déficience technique ou autre. Or, selon l'article L.133-19 V. du code précité, le payeur ne doit supporter aucune conséquence financière si l'opération de paiement non autorisée a été effectuée sans que le prestataire de services de paiement du payeur n'exige une authentification forte du payeur prévue à l'article L. 133-44. Cet article est entré en vigueur au moment de la mise en place de ladite authentification forte, l'ACPR en ayant rappelé l'exigence le 26 avril 2021.

Je rappelle que les commerçants doivent supporter ce risque au titre de l'article L.133-19 VI du même code et émettre un « impayé » en cas de contestation de paiements par les titulaires de cartes bancaires.

Enfin, j'indique que l'article L.133-17 du même code dispose que l'utilisateur de services de paiement est tenu de signaler une opération de paiement non autorisée sans tarder. Je constate à ce titre la contestation tardive des paiements frauduleux par Monsieur X, laquelle révèle un défaut de vigilance de sa part. Je lui rappelle donc qu'il lui appartient de consulter régulièrement et attentivement ses relevés de comptes afin d'être en mesure de contester toute opération anormale ou irrégulière avec toute la célérité requise.

Les conclusions de la Médiatrice

Ainsi, je propose à la Banque de rembourser Monsieur X des paiements effectués après le 26 avril 2021 au titre de l'article L 133-19 V et l'invite à se retourner ensuite auprès des commerçants concernés, au titre de l'article L.133 19 VI.

Pour les opérations effectuées avant le 26 avril 2021, je propose qu'elles fassent l'objet d'un partage de responsabilité entre Monsieur X, (en application de l'article L.133-17 et L.133-24 précités) et la Banque (conformément aux articles L 133-19 II et L.133-23). ◆

La perte de chance liée à l'intrusion frauduleuse dans l'espace bancaire en ligne



François

Les faits

Madame X souhaite obtenir le remboursement de plusieurs opérations de paiement à distance par carte bancaire, validées en authentification forte.

Elle relate avoir reçu un appel téléphonique d'un individu qui s'est présenté comme un conseiller de sa Banque et l'a informée de plusieurs achats en cours sur son compte bancaire. Il a demandé à Madame X de les valider grâce à son application bancaire, pour qu'il les annule.

Mise en confiance par le discours de son interlocuteur qui semblait tout connaître de sa situation bancaire, Madame X a suivi ses instructions et a validé les achats.

Lorsqu'elle a constaté le débit des paiements qu'elle pensait annuler, elle en a demandé le remboursement à sa Banque.

L'analyse de la Médiatrice

Les faits énoncés par Madame X semblent révéler une escroquerie qui a pris la forme d'un « vishing ». C'est une technique utilisée pour obtenir frauduleusement des informations confidentielles et/ou faire valider des opérations trompeuses via un appel téléphonique. L'escroquerie relève du droit pénal, toutefois,

en ma qualité de Médiatrice de la consommation, il me revient d'apprécier l'éventuelle responsabilité de la banque dans l'exécution des opérations de paiements contestées.

Ainsi une banque qui refuse le remboursement d'une opération contestée doit prouver :
- que le client réfutant avoir autorisé une opération de paiement a agi frauduleusement ou a fait preuve de négligence grave ;
- ou que le payeur a validé lui-même le paiement et que l'opération a donc été autorisée.

L'établissement était effectivement en droit de ne pas rembourser sa cliente qui a utilisé son application pour valider les paiements sous la pression de l'escroc ; toutefois, j'ai remarqué qu'étonnamment, le fraudeur connaissait parfaitement la situation bancaire de sa victime.

Dès lors j'ai relevé, preuve informatique à l'appui, que le fraudeur avait réussi à récupérer, probablement via un phishing préalable, les accès de l'application bancaire en ligne de Madame X, et s'y était connecté au moment de l'appel téléphonique. Cela lui a permis de connaître des informations confidentielles rendant d'autant plus crédible son escroquerie. Il en a aussi profité pour relever les plafonds de paiement de sa carte.

Or l'article L.133-44 du Code monétaire et financier prévoit que l'authentification forte est requise « *lorsque le payeur (…) 1°Accède à son compte de paiement en ligne … 3° Exécute une opération par le biais d'un moyen de communication à distance, susceptible de comporter un risque de fraude en matière de paiement ou de toute autre utilisation frauduleuse* ».

Une authentification forte est la réunion d'au moins deux des trois critères suivants :
- un élément de connaissance, c'est-à-dire ce que seul le client connait, tel un mot de passe, une question ou code secret, etc. ;
- un élément de possession, ce que seul le client possède, un téléphone portable par exemple ;
- un élément d'inhérence biométrique, c'est ce qu'est le client, comme l'utilisation de la reconnaissance faciale, vocale ou de l'empreinte digitale.

L'authentification forte lors de chaque connexion à l'espace bancaire en ligne est donc imposée par la Loi, et la possibilité de ne requérir cette authentification que tous les 90 jours résulte d'un règlement délégué de la Commission européenne, lequel ne s'applique que lorsque l'accès est limité aux consultations du solde et des mouvements antérieurs.

Je considère que cette tolérance n'empêche pas les établissements de réauthentifier systématiquement l'accès au compte en ligne, lorsque la connexion se fait grâce à un appareil inhabituel.

Les conclusions de la Médiatrice :

Madame X a participé à la réalisation de son préjudice en compromettant la confidentialité de son code d'accès à son espace bancaire, puis en validant elle-même les opérations, comme le démontrent les pièces informatiques, ce qui ne lui donne pas droit à un remboursement de la part de sa Banque.

J'estime néanmoins que si le fraudeur avait dû obtenir de Madame X qu'elle l'autorise explicitement à se connecter à son application bancaire, celle-ci, plus méfiante, aurait pu comprendre la tromperie : pourquoi un collaborateur de banque aurait-il besoin de pénétrer dans son espace bancaire alors qu'il prétendait observer les mouvements sur son compte ?

Cela a donc entrainé une perte de chance pour Madame X, l'empêchant de s'apercevoir de l'escroquerie dont elle était victime. En outre, le relèvement de son plafond carte a aggravé son préjudice.

Par conséquent, l'absence de vérification par authentification forte, à l'occasion d'une connexion à l'espace en ligne et à partir d'un terminal inconnu, constitue, selon moi, un défaut d'application de l'article L 133-44, qui engage la responsabilité de la Banque.

J'ai proposé un geste, proportionné aux responsabilités de chaque partie. ◆

Intrusion frauduleuse dans la banque en ligne



Chloé

Les faits

Monsieur et Madame X relatent avoir reçu un appel, provenant d'un numéro identique à celui de leur banque, leur interlocuteur se présentant comme un nouveau conseiller de leur agence. En raison du départ récent de leur conseillère attitrée, la situation leur paraissait donc cohérente.

Lors de cet appel frauduleux, le prétendu conseiller prétexta une suspicion de fraude sur leur compte bancaire, et leur indiquait qu'il fallait immédiatement suivre une procédure pour mettre les cartes bancaires en opposition.

Pour Monsieur et Madame X, tout portait à croire qu'il s'agissait d'un collaborateur de leur banque : le fraudeur était informé de virements effectués sur leur compte, dont ils n'étaient pas à l'initiative, et connaissait des informations qui leur étaient personnelles. Comme ils se montraient soupçonneux et refusaient de communiquer leurs codes d'authentification forte par téléphone, le fraudeur a rétorqué en les orientant vers leur messagerie sécurisée à laquelle seul un conseiller de la banque pouvait avoir accès, où ils ont effectivement renseigné les deux codes.

Je comprends de ces faits que le fraudeur avait accès à l'espace en ligne des clients avant même de les avoir au téléphone, qu'il connaissait leur identifiant ainsi que leur code personnel.

La banque de son côté argue que les opérations, validées par authentification forte par deux codes, (procédure du SMS renforcé) ne pouvaient avoir été réalisées que par la saisie du code à usage unique que Madame X avait reçu par SMS sur son téléphone et du code personnel qu'elle est la seule à connaitre (et qui ne circule pas par messagerie). Cela constituait pour l'établissement bancaire une négligence grave de ses clients, l'exonérant de toute responsabilité.

L'analyse de la Médiatrice

J'ai dans un premier temps évoqué la jurisprudence constante, faisant peser sur la banque qui refuse un remboursement d'opérations contestées, la charge de prouver que son client qui réfute avoir autorisé une opération de paiement, a agi frauduleusement ou n'a pas satisfait intentionnellement ou par négligence grave à ses obligations découlant notamment de l'article L.133-16 du Code monétaire et financier.

J'ai noté que Monsieur et Madame X avaient communiqué les données de leur carte bancaire et codes d'authentification au fraudeur par la messagerie sécurisée de leur espace personnel.

Dans un second temps, j'ai relevé que le fraudeur avait nécessairement dû se connecter à l'espace en ligne à partir d'un autre terminal que celui ou ceux à partir du ou desquels Monsieur et Madame X se connectent habituellement. Or, les pièces transmises par la banque n'indiquaient pas que la connexion du fraudeur avait fait l'objet d'une authentification préalable. Dès lors, cette absence d'authentification forte à l'occasion de cette connexion à partir d'un terminal inconnu constituait un défaut d'application de l'article L.133-44 du Code monétaire et financier.

J'ai en effet considéré que cela avait entrainé une perte de chance pour Monsieur et Madame X de ne pas divulguer au fraudeur leurs codes et informations de carte bancaire par la messagerie sécurisée de leur espace client, persuadés que seul un conseiller pourrait avoir accès à ce mail.

La conclusion de la Médiatrice

J'ai constaté que la responsabilité de la banque ne pouvait être engagée sur le refus de remboursement des paiements, validés en authen-

tification forte par un escroc, à la suite de la compromission des données de sécurité personnalisées de Monsieur et Madame X.

Toutefois, le défaut d'authentification préalable lors de l'accès de l'escroc à leur espace bancaire ayant manifestement causé une importante perte de chance pour Monsieur et Madame X, aboutissant à la saisie de leurs deux codes sur leur messagerie sécurisée, j'ai considéré qu'il y avait une responsabilité partagée et proposé de leur rembourser la moitié de leurs pertes. ◆

Virements frauduleux



Gizem

Les faits

Madame X a demandé le remboursement de trois virements d'un montant total de 1950€. De plus, elle a précisé qu'un virement interne de 2000€ a été réalisé quelques minutes avant la première opération contestée.

Madame X a reçu un appel téléphonique d'une personne se présentant comme un collaborateur du service fraude de son établissement bancaire, l'informant de plusieurs opérations douteuses sur son compte. Son interlocuteur lui a envoyé des liens par SMS afin de bloquer ces opérations. Madame X a admis avoir «validé un lien» envoyé par son interlocuteur.

La banque argue que les virements ont été réalisés à la suite de la création d'un nouveau bénéficiaire sur l'espace en ligne de Madame X et que cet ajout a été validé par authentification forte.

L'analyse de la Médiatrice

Des pièces fournies par la Banque, j'ai constaté que l'authentification forte n'a été utilisée qu'une seule fois, à l'occasion de la seule validation de l'ajout d'IBAN. Aucun des trois virements n'a donc fait l'objet d'une revalidation par une authentification complémentaire.

Or, la réglementation applicable en la matière dispose que les paiements ordonnés vers un bénéficiaire de confiance, après que ce bénéficiaire a été désigné et validé par authentification forte lors de son ajout sur l'espace en ligne, ne dispensent pas la banque de demander une authentification des paiements ultérieurement effectués en faveur de ce même bénéficiaire.

En outre, une jurisprudence récente (arrêt du 30 novembre 2022 n° 21-17.614 à propos d'un retrait DAB) rappelle en effet qu'une opération de paiement n'est autorisée que si **son montant** a été validé par le payeur.

Je considère que ce défaut d'authentification lors de la réitération des deux virements qui ont suivi l'exécution du premier engage alors la responsabilité de la Banque.

Concernant le virement interne, le fraudeur a nécessairement dû se connecter à l'espace en ligne à partir d'un autre terminal que celui ou ceux à partir du ou desquels Madame X se connecte habituellement. Je rappelle que l'article L.133-44 du code monétaire et financier **prévoit que l'authentification forte est requise** «*lorsque le payeur (…) Accède à son compte de paiement en ligne*».

La connexion découle nécessairement de la compromission des données de sécurité personnalisées de Madame X, dont la responsabilité est incontestable puisqu'elle est la seule à connaitre son code d'accès.

En revanche, l'absence de vérification par authentification forte à l'occasion de cette connexion à l'espace en ligne à partir d'un terminal inconnu constitue **un défaut d'application de l'article L 133-44, qui engage la responsabilité de la Banque.** Cela a clairement entrainé **une perte de chance** pour Madame X,

l'empêchant de s'apercevoir dès son origine de l'escroquerie dont elle a été victime.

En validant uniquement «le lien» Madame X a confirmé par une seule authentification, après l'intrusion malveillante, l'enregistrement de l'IBAN et les trois virements successifs.

La conclusion de la Médiatrice

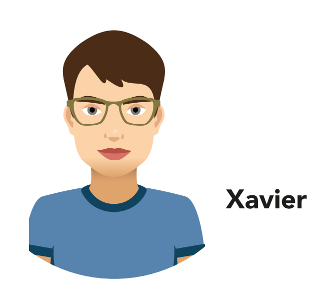
Je ne peux retenir une quelconque responsabilité de la banque dans le déroulement de cette escroquerie, alors que celle de Madame X est pleinement engagée dans la compromission de ses données de sécurité personnalisées et par sa validation de l'enregistrement de l'IBAN frauduleux.

En revanche, **la responsabilité de la banque est engagée à deux titres :**

- celui du défaut d'authentification forte lors de la connexion du fraudeur à l'espace en ligne de Madame X
- celui du défaut d'autorisation explicite du montant des virements, exécutés sans authentification complémentaire dès que les ordres ont été passés.

Je considère que les responsabilités sont partagées et je propose que la banque rembourse à Madame X la moitié de son préjudice. ◆

Fraude au RIB intercepté pour un virement vers un notaire



Xavier

Les faits

Dans le cadre d'un acte notarié de donation à ses enfants, Monsieur X devait effectuer un virement d'un montant important à son notaire. Pour ce faire, le notaire lui a transmis par mail un RIB semblant être celui de la Caisse des Dépôts et Consignations (CDC), que Monsieur X a ensuite transféré à sa conseillère bancaire afin qu'elle puisse réaliser le virement.

Or, les échanges de mails entre le client et le notaire ont été interceptés par un fraudeur qui a ensuite usurpé l'identité du notaire et modifié l'IBAN figurant sur le RIB transmis à Monsieur X.

En somme, le virement a été effectué au profit du compte du fraudeur en lieu et place du compte du notaire, c'est pourquoi Monsieur X demandait le remboursement du virement litigieux.

L'analyse de la Médiatrice

Au préalable, j'ai rappelé aux parties la réglementation en matière d'opérations de paiement, puis j'ai constaté que le virement était une opération autorisée au sens du Code monétaire et financier.

J'ai ensuite relevé que la Banque avait procédé à l'exécution du virement conformément à l'article L.133-21 du Code monétaire et financier, et que l'opération présentait toutes les caractéristiques d'une opération régulière dans la mesure

où l'ordre de virement avait été donné par Monsieur X à destination du compte apparaissant sur le RIB, qu'il avait lui-même transmis par courriel.

J'ai ensuite souligné que par application du principe de non-immixtion, la jurisprudence constante ne met pas à la charge de la banque la vérification de la concordance entre le nom du destinataire du virement et l'intitulé ou la qualité du titulaire du compte dont le donneur d'ordre a fourni l'identifiant (IBAN), ceci relevant de la seule responsabilité du payeur.

Toutefois, j'ai précisé que le principe de non-immixtion s'articule avec celui de vigilance, qui incombe au banquier, qui doit procéder à certaines vérifications pour détecter les anomalies apparentes ou irrégularités manifestes.

Or, Monsieur X ayant informé la banque a plusieurs reprises quant au bénéficiaire de son virement, cette dernière ne pouvait ignorer l'objet de ce virement et surtout la destination des fonds. Dès lors, j'ai considéré que la Banque aurait dû remarquer que le BIC n'était pas celui de la Caisse des Dépôts et Consignations; il s'agissait d'une incohérence manifeste, en tout cas d'une anomalie apparente.

Les conclusions de la Médiatrice

La Banque n'engage pas sa responsabilité en refusant de prendre en charge la fraude découlant d'une falsification d'IBAN; toutefois s'agissant d'un virement explicitement destiné à un notaire, je relève l'insuffisante vigilance de la Banque, qui n'a pas repéré l'incohérence manifeste entre le BIC fourni et la domiciliation attendue du compte du notaire auprès de la Caisse des Dépôts et Consignations. J'ai donc proposé un geste de réparation très conséquent. ◆

Chèque intercepté et falsifié



Soraya

Les faits

Monsieur X a émis un chèque dont l'ensemble des champs étaient renseignés et l'a adressé par voie postale au bénéfice du Centre des finances publiques de sa ville de résidence.

Bien que son chèque ait été débité de son compte bancaire dix jours plus tard, il a reçu une relance de l'administration fiscale qui lui indiquait ne pas avoir reçu le paiement. Monsieur X a alors demandé à sa Banque, dite «Banque tirée», une copie du chèque émis.

Après plusieurs relances, la Banque tirée a envoyé une copie de ce chèque, quatre mois plus tard. Monsieur X a découvert que le libellé du chèque avait été falsifié et soulevait que l'écriture utilisée était très différente de la sienne.

Monsieur X a donc porté plainte et en parallèle demandé à sa Banque le remboursement du chèque falsifié.

La Banque tirée a répondu que le remboursement dépendait de la Banque réceptrice et qu'il n'y avait pas de certitude que les fonds puissent être remboursés puisque la réclamation de Monsieur X datait de plus de deux mois après son encaissement.

Néanmoins, Monsieur X ne pouvait pas faire de réclamation plus tôt puisqu'il avait attendu que l'administration fiscale le relance, puis encore quatre mois pour que sa Banque lui envoie la copie du chèque falsifié.

L'analyse de la Médiatrice

Mon analyse s'est portée sur deux points : le délai d'obtention de la copie du chèque et l'obligation de contrôle de la régularité formelle du chèque par la Banque.

En premier lieu, Monsieur X regrettait que la Banque ait tardé, malgré ses relances, à envoyer la copie du chèque.

Sur ce point, les banques utilisent un système d'image-chèque qui consiste à scanner les chèques et de les archiver de façon numérique.

En l'espèce, la Banque a tardé à envoyer la copie du chèque, ce qui n'a pas permis à Monsieur X d'effectuer une réclamation pendant le délai imposé de deux mois par la Banque.

Si la Banque avait envoyé la copie rapidement, Monsieur X aurait pu se rendre compte rapidement de la fraude et faire une réclamation dans les délais impartis.

En second lieu, Monsieur X mettait en cause l'absence de vérification de la Banque tirée sur le chèque.

Le chèque est un mandat de payer qui doit, au titre de l'article L.131-2 du Code monétaire et financier, comporter des mentions obligatoires : le nom du bénéficiaire, le montant, la date ainsi que la signature de la personne qui émet le chèque.

En application de l'article 1937 du Code civil, en l'absence de faute du déposant, et même si la Banque n'a pas commis de faute, cette dernière n'est pas libérée envers son client qui lui a confié les fonds sur présentation d'un ordre de paiement, revêtu dès l'origine d'un faux.

La jurisprudence française indique de façon constante que le banquier est tenu de prouver que l'ordre de paiement n'était pas affecté d'une anomalie apparente décelable par un employé de banque normalement diligent.

La Cour de cassation a par ailleurs affirmé que la banque doit relever les anomalies apparentes et assumer les conséquences des risques qu'elle prend en s'en abstenant.

En l'espèce, la Banque n'avait pas prouvé que le chèque n'était pas affecté d'une anomalie apparente. Pourtant, le chèque tel qu'il m'a été présenté contenait une différence entre l'écriture du libellé, qui avait été falsifié, et le reste des informations, écrites par Monsieur X dès son émission.

Par conséquent, les écritures étaient clairement dissemblables. Il s'agissait bien d'une anomalie apparente.

Les conclusions de la Médiatrice

En conclusion, au vu de la différence d'écritures notable, la Banque tirée aurait dû rejeter le chèque. Par ailleurs, cette dernière n'a pas cherché à apporter la preuve de l'absence d'anomalie apparente et n'a pas justifié valablement le délai qui s'était écoulé entre la demande de copie du chèque par Monsieur X et sa réception effective.

J'ai considéré que cela engageait la responsabilité de la banque tirée et de la banque présentatrice, sur le fondement de leur obligation de contrôle de la régularité formelle du chèque.

Par ailleurs, le délai de deux mois résulte de conventions interbancaires et n'est pas opposable aux émetteurs de chèques, en pareilles circonstances.

En conclusion, j'ai proposé à la Banque tirée de lui rembourser les fonds. ◆

Utilisation frauduleuse d'un chèque de banque



Ophélia

Les faits

Dans l'optique de la vente de son véhicule, Monsieur T prévient l'acheteur que celle-ci s'effectuera au moyen d'un chèque de banque. Pour ce faire, quelques jours avant la vente, afin de faire les vérifications d'usage et s'assurer de la conformité du chèque, Monsieur T demande à l'acheteur de lui envoyer par SMS la photo dudit chèque. A la réception dudit message, Monsieur T contacte l'Agence bancaire émettrice du chèque, qui lui confirme sa conformité.

Le jour de la transaction, Monsieur T effectue de nouveau des vérifications pour s'assurer que le chèque remis par l'acheteur correspond bien à celui de la photographie envoyée quelques jours plus tôt et vérifié auprès de l'Agence émettrice (numéro de chèque, date, signature, destinataire, le logo du chèque au dos). Ne constatant rien d'anormal, Monsieur T procède à la vente du véhicule. Un jour après, Monsieur T dépose ledit chèque sur son compte et les fonds lui sont crédités. Deux jours plus tard le montant est débité de son compte, le chèque étant revenu impayé. Se déplaçant à son Agence, Monsieur T est informé que le chèque remis à encaissement était un faux et que le véritable chèque de banque émis par l'Agence émettrice avait été mis en opposition.

Monsieur T a donc demandé à sa Banque la restitution du montant du chèque qui lui avait été initialement crédité. Confronté à un refus, il me saisit en faisant valoir s'être assuré de la conformité du chèque de banque, qui s'est toutefois avéré faux.

L'analyse de la Médiatrice

Bien qu'ayant fait preuve de prudence en effectuant certaines vérifications et en s'assurant de la validité et de la conformité du chèque préalablement à sa remise, la Banque de Monsieur T précise que celui-ci n'a pas demandé d'avis de sort et n'a pas vérifié la présence du filigrane.

Je rappelle alors que par le biais d'un avis de sort, la banque du bénéficiaire du chèque peut interroger la banque émettrice du chèque, avant son encaissement, afin de s'assurer de la provision d'un chèque. Toutefois lors de l'émission d'un chèque de banque, un avis de sort n'est, généralement, pas pertinent dès lors que le chèque de banque obtenu par l'acheteur auprès de sa banque a la particularité d'être débité sur le compte de l'établissement bancaire émetteur du chèque et non sur celui de l'acheteur.

Pour lutter contre les faux chèques de banque, la Place bancaire française a introduit l'obligation pour les chèques de banque de comporter un filigrane normalisé identique pour toutes les banques. Facile à reconnaître à l'œil nu, par transparence, il couvre une partie importante de la surface du chèque et comporte la mention « CHÈQUE DE BANQUE » lisible au dos du chèque. Je précise que cette mention est bordée en haut et en bas par deux semeuses, dont les parties claires et sombres du dessin de l'une sont inversées par rapport à celles de l'autre. Je souligne que cette vérification peut être faite par le bénéficiaire du chèque mais cette tâche incombe, néanmoins, principalement et essentiellement à la banque auprès de laquelle le chèque est déposé.

La vérification de la présence du filigrane n'ayant pas été opérée, puisque le chèque remis à Monsieur T a été présenté au paiement par sa Banque alors qu'il s'est avéré faux, constituait donc un manquement de la part de celle-ci.

Néanmoins, ce manquement n'a été ni la cause ni à l'origine du préjudice car le chèque a été

déposé à l'encaissement après que la vente avait eu lieu. Ainsi même si cette vérification avait été faite, cela n'aurait manifestement pas pu déjouer l'escroquerie car Monsieur T n'était déjà plus en possession de son véhicule au moment de la remise du chèque : le préjudice était déjà constitué car la voiture avait été remise à l'escroc.

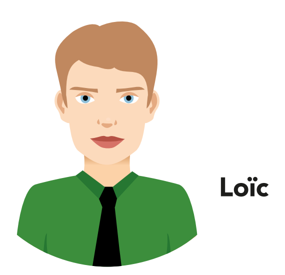
En outre, conformément à la convention de compte, la Banque a la possibilité de contre-passer au débit le montant d'un chèque, provisoirement crédité sur le compte, si celui-ci revient impayé ; tel est le cas en l'espèce. Je rappelle également dans la mesure où le chèque de banque remis à l'encaissement était un faux, celui-ci était « vide » car aucune provision n'existait et n'était rattachée audit chèque. Celui-ci constituait en tout état de cause un morceau de papier sans aucune valeur légale ni fiduciaire.

Que ce soit la banque teneuse de compte ou la banque émettrice du chèque, aucune d'elles n'est tenue d'honorer un faux chèque ; d'autant plus que le véritable chèque de banque a été mis en opposition avant que Monsieur T ne dépose le faux chèque sur son compte.

Les conclusions de la Médiatrice

La banque n'engage pas sa responsabilité en refusant le remboursement d'un chèque de banque frauduleux ; toutefois j'ai relevé un manquement à la réglementation puisqu'elle n'a pas vérifié le filigrane normalisé avant présentation au paiement, ce qui a fait l'objet d'une proposition de geste financier. ◆

Retrait à un distributeur automatique de billets



Loïc

Les faits

Alors que Madame X a inséré sa carte bancaire au sein d'un distributeur en agence afin d'effectuer un retrait, elle a été abordée par un individu qui lui a indiqué que le distributeur ne fonctionnait pas. Elle a donc suivi ses instructions et récupéré sa carte avant de quitter les lieux. Plus tard, elle a constaté qu'un retrait de 500 € avait été débité de son compte et en a demandé le remboursement.

La Banque refuse le remboursement au motif que la transaction ne présente aucune irrégularité et a été autorisée dans le respect des procédures de sécurité en vigueur : utilisation physique de la carte, lecture de la puce infalsifiable et validation par le code confidentiel.

L'analyse de la Médiatrice

Je rappelle que la médiatrice n'est pas compétente pour connaitre des escroqueries.

Il résulte d'un arrêt de la Cour de cassation du 30 novembre 2022 (n° 21-17.614) qu'une opération de paiement « *initiée par le payeur, qui donne un ordre de paiement à son prestataire de services de paiement, est réputée autorisée uniquement si le payeur a également consenti au montant de l'opération.* » Ainsi, il ne suffit pas que le titulaire ait introduit sa carte dans le distributeur et composé le code pour que l'opération soit autorisée, encore faut-il qu'il ait composé le

montant du retrait souhaité, avant de saisir son code confidentiel, cette validation par le code attestant qu'il a bel et bien autorisé ce montant.

En l'occurrence, le script des automates de la Banque prévoit que le montant demandé soit saisi avant la composition du code. Par conséquent, il s'agit d'une opération autorisée au sens de l'arrêt susvisé. Je constate par ailleurs qu'il n'est fait mention d'aucun ticket d'abandon de retrait.

En outre, le fait d'avoir tenté d'effectuer ce retrait au vu et au su d'un tiers, vraisemblablement en suivant ses instructions, est révélateur d'une imprudence pouvant être qualifiée de négligence grave.

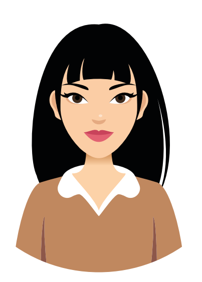
Les conclusions de la Médiatrice

Les modalités du retrait impliquent donc qu'il s'agit d'une opération autorisée, ce qui fait obstacle à un remboursement.

Toutefois, puisque le vol d'espèces a été réalisé auprès d'un distributeur localisé au sein d'un sas d'une agence, ouverte au moment des faits, j'estime que cela engage la responsabilité de la Banque.

Je propose ainsi un partage de responsabilité entre la Banque et Madame X et préconise un remboursement de la moitié du préjudice soit 250€. ◆

Saisie attribution émise sans que le débiteur saisi en ait été informé



Mélanie

Les faits

Une Saisie Attribution (SA) concernant Monsieur X, a été notifiée à la banque, par voie dématérialisée. Monsieur X reproche à la banque de ne pas lui avoir transmis l'acte de saisie, il conteste également la mise à disposition du Solde Bancaire Insaisissable (SBI) et le montant des frais prélevés par la banque, lors du traitement de cette SA.

L'analyse de la Médiatrice

La SA est régie aux articles L.211-1 à L.211-5 et R.211-1 à R.211-23 du Code des procédures civiles d'exécution (CPCE). La loi Justice du 23 mars 2019, prévoit la dématérialisation des échanges entre huissiers de justice et banques depuis le 1er avril 2021, suivant l'article L.211-1-1 du CPCE. En outre, le décret n° 2019-992 du 26 septembre 2019 prévoit qu'en cas de signification de la saisie par voie électronique, la banque doit communiquer à l'huissier, par la même voie, au 1er jour ouvré suivant la signification, les informations relatives à ses obligations à l'égard du débiteur, selon l'article R.211-4 du CPCE. De plus, l'article R.211-3 du CPCE, prévoit qu'à peine de caducité, la saisie est dénoncée au débiteur par acte d'huissier sous 8 jours. Le débiteur peut contester la saisie suivant l'article R.211-10 du CPCE.

S'agissant du SBI, en vertu des articles 2284 du Code civil et L.112-1 du CPCE, tous les biens

sont saisissables en principe. Par exception, des biens peuvent être déclarés insaisissables.

L'article L162-2 du CPCE prévoit que le tiers saisi laisse à disposition du débiteur, personne physique, un solde à caractère alimentaire égal au montant du Revenu de Solidarité Active (RSA), mentionné à l'article L.262-2 du Code de l'action sociale et des familles. Le SBI est laissé automatiquement à disposition du débiteur conformément à l'article R.162-2 du CPCE. L'article R.162-6 du CPCE ajoute que le débiteur saisi doit demander la mise à disposition des sommes insaisissables, avant que le créancier n'ait sollicité le paiement des sommes saisies.

Enfin, Monsieur X a contesté les frais de traitement de la SA prélevés par la banque.

Les conclusions de la Médiatrice

J'observe que le débiteur saisi peut contester la SA, mais qu'il ne l'a pas fait au cas d'espèce. Je considère que la banque ne pouvait remettre à Monsieur X une copie de la SA, ayant reçu la notification par voie dématérialisée. J'estime qu'il revenait à l'huissier de dénoncer la SA au débiteur sous 8 jours, suivant la signification de l'acte. Monsieur X m'a expliqué ne pas être parvenu à contacter l'huissier. J'ai donc appelé l'étude d'huissier et j'ai appris que son dossier était archivé, toutefois l'étude m'a communiqué un numéro à contacter, que j'ai transmis au débiteur saisi, pour qu'il puisse obtenir une copie de l'acte tel que souhaité.

S'agissant du SBI, j'observe que la banque a tenu compte du SBI en le déduisant des sommes déclarées au créancier saisissant et le montant a été laissé en intégralité à Monsieur X.

Concernant les frais prélevés, ils sont prévus au guide tarifaire de la banque, aussi, je considère qu'ils ne sont pas injustifiés. ◆

Changement de bénéficiaire d'un contrat d'assurance vie



Christelle

Les faits

La fille de Madame X souhaitait que la Banque modifie la clause bénéficiaire des contrats d'assurance-vie souscrits par sa mère, sur la base d'une procuration notariée qui la mandatait pour modifier ladite clause conformément aux dispositions contenues dans un testament rédigé 6 ans auparavant par Madame X et déposé chez un notaire.

La Banque, en accord avec l'assureur, avait déjà refusé 6 ans auparavant de modifier la clause bénéficiaire, car Madame X, interrogée par son agence, n'avait pas été en mesure de confirmer les dispositions prises dans le testament, et que la signature ne semblait pas être la sienne.

La Banque maintenait donc cette position de ne pas modifier la clause bénéficiaire, au motif que l'assureur refusait que ce droit exclusif du souscripteur soit exercé par un tiers.

La fille de Madame X soulevait de son côté que sa mère avait le droit de disposer de son contrat d'assurance à sa convenance, et qu'elle n'avait fait que suivre les indications de son agence en demandant au notaire un mandat aux fins de modifier la clause bénéficiaire.

L'analyse de la Médiatrice

M'étant reportée au testament contenant les dispositions relatives au changement de bénéficiaire d'assurance-vie, j'ai pu constater qu'il

s'agissait bien d'un testament olographe et non d'un testament notarié. Le notaire à qui il avait été remis à titre de conservation n'était donc pas présent lors de sa rédaction et sa signature, il ne pouvait donc s'engager sur son authenticité et sa bonne compréhension par Madame X.

J'ai comparé la signature portée sur cet acte avec la signature de Madame X apposée sur la procuration notariée et sur le mandat de représentation qu'elle avait signé pour me saisir et, sans être graphologue, j'ai pu constater que la signature apposée sur le testament était éloignée de ces deux autres signatures concordantes.

J'ai donc considéré que la position de la Banque, dans un contexte où sa cliente n'avait pas été en mesure de lui confirmer ses volontés lors d'un entretien, était une position de prudence au regard de la jurisprudence, et qu'il ne pouvait lui être reproché d'avoir refusé de prendre le risque de modifier la clause sur la base d'un acte possiblement entaché de nullité.

J'ai également rappelé les articles L.133-8 et L.132-9 du Code des assurances en application desquels la désignation et la révocation d'un bénéficiaire est un droit personnel du souscripteur.

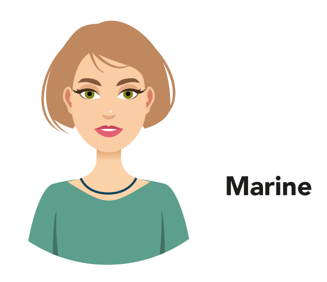
Enfin, j'ai précisé que la Banque n'est pas partie au contrat d'assurance, et qu'il ne peut lui être reproché, en sa qualité de mandataire de l'assureur, d'appliquer les directives de ce dernier.

Les conclusions de la Médiatrice

En conséquence, j'ai considéré que je ne pouvais demander à la Banque et à l'assureur d'accepter de modifier la clause bénéficiaire en application de la procuration notariée, et j'ai invité la fille de Madame X à se rapprocher de l'assureur, pour connaître les conditions dans lesquelles il accepterait une modification de la clause du contrat d'assurance-vie par Madame X.

J'ai toutefois estimé que la Banque n'avait pas été assez explicite sur l'acte notarié dont l'assureur avait besoin pour faire les modifications, ce qui avait donné lieu à la remise et facturation d'un acte qui ne lui convenait pas, et dont elle devait prendre en charge le coût. ◆

Mise en jeu de l'assurance attachée à la carte bancaire dans le cadre des aléas engendrés par la crise sanitaire



Marine

Les faits

Monsieur X m'a saisie en déplorant la non prise en charge par l'assurance associée à sa carte bancaire des frais du voyage qu'il avait dû annuler.

Il demandait donc le remboursement de la somme de 1600€ au motif qu'il n'avait pas eu communication de l'exclusion de garantie liée au COVID de l'assurance de sa carte bancaire avec laquelle il avait réglé ce voyage en famille, au bord d'un joli lac aux pierres rouges de l'Hérault.

En effet, testé positif au COVID la veille du départ, son voyage avait été annulé, mais non remboursé faute d'une assurance annulation. Il avait contacté le service carte qui lui avait indiqué que le montant du voyage était perdu, la carte ne couvrant pas le covid. Il déplorait ne pas en avoir été informé par sa banque estimant qu'il aurait dû être prévenu de ces nouvelles dispositions.

La Banque Y m'a expliqué qu'il n'avait pas été possible de faire jouer l'assurance incluse dans la carte en faisant valoir que la notice d'information de l'assurance de cette carte exclut des garanties proposées les cas d'épidémie et de pandémie.

Elle soulignait également que Monsieur X, avant de prendre la décision de refuser l'assurance annulation proposée par son prestataire de voyage, aurait dû prendre la précaution de vérifier l'état de la couverture assurance de la carte, et qu'il pouvait à l'époque, outre la consultation du site dédié, se rapprocher directement de son agence pour obtenir les informations nécessaires.

L'analyse de la Médiatrice

J'ai pris connaissance de la notice d'information du contrat d'assurance transmise et y ai lu que l'épidémie et la pandémie font partie des causes d'exclusions communes. Il n'y avait donc pas de doute sur le fait que Monsieur X n'était pas couvert, la question étant celle de la suffisance ou non de l'information.

J'ai relevé que la notice d'assurance est disponible sur demande auprès des conseillers mais également sur le site internet en indiquant le numéro de carte, ainsi que je l'ai moi-même vérifié. Il en ressort donc clairement que Monsieur X aurait été en mesure de vérifier la couverture exacte de son assurance.

La conclusion de la Médiatrice

Bien que je regrette la situation dans laquelle s'était trouvé Monsieur X, je n'ai pas relevé de responsabilité de la banque dans le non-remboursement de ses frais de vacances annulées.

J'ai estimé toutefois, en équité, que la Banque aurait pu communiquer plus largement, auprès de tous ses clients détenteurs de cartes de même niveau, sur ces exclusions, postérieurement aux périodes COVID. Cette pandémie a revêtu un caractère exceptionnel alors que les voyageurs accoutumés à se sentir protégés par leurs cartes bancaires ne pouvaient anticiper ce besoin de couverture supplémentaire pour des déplacements en France.

Ainsi, j'ai proposé un geste au titre de la nécessaire information générale que la période post COVID rendait utile. ◆

Crédit à la consommation : Confusion entre une carte à débit différé et un crédit renouvelable



Stanislas

Les faits

Madame X a constaté que des intérêts lui étaient prélevés, alors que sa carte bancaire prévoit un débit différé sans surcoût. Elle me saisit afin d'obtenir le remboursement de ces sommes.

La banque indique que Madame X détient une carte bancaire à débit immédiat ainsi qu'un crédit renouvelable assorti d'une carte de crédit et suppose que Madame X a confondu ces deux cartes.

L'analyse de la Médiatrice

Je rappelle que conformément à l'article L.312-57 du Code de la consommation, un crédit renouvelable est un crédit à la consommation dont l'utilisation est facilitée. Une fois le montant maximum de crédit déterminé, l'emprunteur peut le mobiliser comme il le souhaite, par virement mais également grâce à la carte de crédit assortie. L'utilisation de ce crédit entraîne des intérêts, conformément au taux prévu par le contrat.

J'ai pu constater que Madame X avait effectivement signé une offre de crédit renouvelable en 2005.

Il s'avère que le prélèvement du crédit renouvelable avait lieu le 7 de chaque mois, cela a

pu entraîner une confusion avec les opérations d'une carte à débit différé.

Néanmoins, Madame X recevait mensuellement des relevés de compte concernant son crédit renouvelable, mentionnant notamment le montant maximum du crédit, le montant disponible, le montant dû et l'estimation du nombre de mensualités restant dues. Madame X ne pouvait donc pas ignorer qu'elle s'était engagée au titre d'un crédit renouvelable qu'elle remboursait tous les mois.

Malgré la mise en opposition à sa carte bancaire, en agence, Madame X ne semblait toujours pas avoir compris qu'elle était engagée au titre d'un crédit renouvelable et ne disposait pas d'une carte à débit différé. À la lecture des relevés de compte, je relève que Madame X mobilise le crédit renouvelable au quotidien, y compris pour des faibles montants, ce qui est surprenant au regard du coût d'un crédit renouvelable. Je constate qu'elle n'a pas compris l'utilité d'une telle ligne de crédit ni comment l'utiliser.

Je considère donc que, la banque a fait preuve d'un défaut d'accompagnement et a vendu à Madame X un produit qui ne lui était pas adapté.

Par ailleurs, il m'apparait que Madame X n'a pas reçu toutes les informations nécessaires au moment de la souscription, notamment les caractéristiques essentielles du crédit proposé, et la fiche précontractuelle d'information.

De plus, l'article L.312-65 du Code de la consommation prévoit une obligation annuelle d'information de l'emprunteur sur les conditions de reconduction du contrat notamment.

En cas de non-respect de ces obligations, le prêteur encourt la déchéance totale ou partielle du doit aux intérêts. Ainsi, il appartient à la banque de prouver avoir satisfait à ces obligations.

Les conclusions de la Médiatrice

J'ai considéré que la banque avait vendu un produit inadapté à Madame X, qui n'était pas au fait des caractéristiques essentielles du crédit renouvelable sur lequel elle s'était engagée, dont elle ne comprenait pas le fonctionnement et ne semblait d'ailleurs pas avoir connaissance de son existence.

J'ai alors invité la banque à rembourser à Madame X la somme due au titre de la réserve utilisée non encore remboursée (839 €). La banque a accepté ce geste. ◆

Durée de validité d'une offre de prêt à la consommation



Ilham

Les faits

Madame X demande une indemnisation correspondant à l'écart de coût entre le prêt avantageux qui lui avait été proposé et celui auquel elle a souscrit.

Une offre de prêt à la consommation à un taux de 1,7 % a été proposée et déposée sur l'espace bancaire en ligne de Madame X pour signature mais elle a souhaité y souscrire sans l'assurance emprunteur, considérant qu'elle n'était pas obligatoire.

Le dossier de Madame X sans assurance emprunteur ayant été refusé par la banque, cette dernière a alors retiré le contrat de prêt de l'espace bancaire en ligne en considérant que l'offre était devenue caduque.

Malgré les demandes de Madame X durant les jours suivants, la banque a refusé maintenir la même offre de prêt à la consommation avec l'assurance emprunteur.

Madame X a finalement accepté de souscrire à une autre offre de prêt à un taux de 2,5 % avec une assurance emprunteur.

L’analyse de la Médiatrice

Tout d’abord, j’ai confirmé que l’assurance emprunteur n’est pas obligatoire pour un crédit à la consommation mais que, dans le cadre de sa politique de risque, un établissement de crédit est parfaitement légitime à exiger la souscription d’une assurance et à refuser le crédit à un emprunteur qui s’y opposerait, ou encore à modifier le taux d’intérêt, estimant que, privé de cette garantie, il prend un risque plus important.

Par la suite, j’ai rappelé que selon l’article L.312-18 du Code de la consommation, « *La remise ou l’envoi de l’offre de contrat de crédit à l’emprunteur oblige le prêteur à en maintenir les conditions pendant une durée minimale de quinze jours à compter de cette remise ou de cet envoi* ».

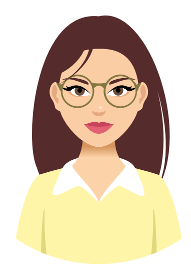
Dès lors, à la lecture de l’article susmentionné *stricto sensu*, il n’est pas permis à la banque de retirer une offre de crédit à la consommation avant la durée minimale de quinze jours.

Aussi, aucun motif ne saurait justifier le retrait d’une offre de crédit à la consommation par la banque avant l’expiration du délai de 15 jours, y compris en cas de refus de l’emprunteur, ce qui n’était pas le cas en l’espèce, s’agissant plutôt d’une tentative de négociation d’une clause par Madame X.

La conclusion de la Médiatrice

J’ai donc considéré que Madame X était fondée à bénéficier de cette offre avant l’expiration du délai légal de 15 jours et j’ai proposé que la banque procède au remboursement du montant correspondant à l’écart de coût entre le prêt à la consommation à taux avantageux qui lui avait été proposé et celui auquel elle a finalement souscrit. ◆

Le non-renouvellement d’un crédit à la consommation à la suite d’une vérification triennale de solvabilité



Olivia

Les faits

Monsieur et Madame X ont souscrit un crédit renouvelable. Celui-ci est défini à l’article L 312-57 du code de la consommation : « *Constitue un crédit renouvelable, une ouverture de crédit qui, assortie ou non de l’usage d’une carte de crédit, offre à son bénéficiaire la possibilité de disposer de façon fractionnée, aux dates de son choix, du montant du crédit consenti* ».

Le contrat de crédit qui a été accordé à Monsieur et Madame X est un crédit d’un montant déterminé et d’une durée d’un an, éventuellement renouvelable. Il s’avère qu’à la suite d’une vérification triennale de solvabilité (VTS) effectuée par la Banque, leur solvabilité étant insuffisante, leur contrat de crédit a donc été résilié.

S’étant vu opposer un refus après avoir sollicité leur agence bancaire afin que leur réserve de crédit soit réactivée, Monsieur et Madame X ont saisi la médiation et souhaitent obtenir des explications justifiant le non-renouvellement de leur crédit à la consommation.

L'analyse de la Médiatrice

Le contrat de crédit renouvelable de Monsieur et Madame X a été mis en place et a fait l'objet d'une vérification triennale de solvabilité. Je comprends que Monsieur et Madame X s'interrogent quant aux conditions de mise en place ou de suspension de ce contrat. Il ressort que, dans le cadre du crédit renouvelable, la banque se devait de vérifier leur solvabilité. En effet, l'article 312-75 du code de la consommation dispose que : « *Avant de proposer à l'emprunteur de reconduire le contrat, le prêteur consulte tous les ans le fichier prévu à l'article L. 751-1, dans les conditions prévues par l'arrêté mentionné à l'article L. 751-6 et, **tous les trois ans, il vérifie la solvabilité de l'emprunteur** dans les conditions fixées à l'article L. 312-16.* ».

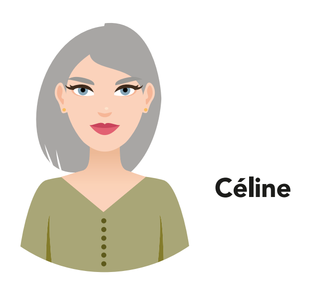
Je rappelle que la solvabilité en droit bancaire s'analyse « à partir d'un nombre suffisant d'informations » qui permettent de définir si un débiteur pourra faire face à ses obligations de remboursement aux échéances fixées dans le cadre du contrat de crédit.

Il s'avère qu'après analyse de la situation de ses clients et des informations en sa possession, la Banque ne pouvait plus se permettre d'octroyer à nouveau un crédit renouvelable à Monsieur et Madame X.

La conclusion de la Médiatrice

En conséquence, je ne relève pas de manquement de la part de la Banque, il ressort de sa responsabilité de vérifier la solvabilité de ses clients-emprunteur. De surcroit, il n'est pas possible d'imposer au banquier qu'il accorde un crédit et ce dernier n'a pas d'obligation de motiver son refus d'octroi d'un crédit. Il s'agit en effet d'une décision souveraine de sa part que la jurisprudence a toujours confirmée. Dans le cas d'espèce, je n'ai pas pu proposer une solution de médiation. ◆

Refus de suspension des mensualités d'un prêt immobilier



Céline

Les faits

Madame et Monsieur X reprochent à la Banque d'avoir refusé leur seconde demande de suspension de mensualités de leur prêt immobilier. Ils estiment avoir été mal conseillés mettant en cause la responsabilité de la Banque.

La Banque rappelle les dispositions contractuelles régissant la demande de suspension des mensualités d'un prêt immobilier, et confirme qu'en raison du contexte sanitaire mondial, elle avait mis en place un système dérogatoire permettant à l'ensemble de sa clientèle, engagée dans le remboursement d'un prêt immobilier, de bénéficier d'une procédure assouplie en cas de demande d'une suspension de mensualités. Néanmoins, le système ayant pris fin, les dispositions contractuelles s'appliquent à nouveau. Or, les clients ne les remplissant pas, la Banque confirme son refus de leur accorder une nouvelle suspension de mensualités.

L'analyse de la Médiatrice

Rappelant les dispositions de l'article 1103 du Code civil, il apparaît que Madame et Monsieur X ne remettent pas en cause le contrat de prêt immobilier signé avec la Banque. Les dispositions contractuelles prévoient la possibilité de demander une ou plusieurs suspensions de mensualités, pour une période maximum de 12 mois, par période minimale fixe, chaque demande ne pouvant être effectuée qu'après l'expiration d'un délai minimal précisément annoncé.

Le système dérogatoire, permettant de lever les contraintes contractuelles pour bénéficier d'une suspension de mensualités, avait été mis en place à titre temporaire par la Banque, pour répondre à l'impératif de crise sanitaire mondiale, il n'avait donc pas vocation à perdurer dans le temps. Il prévoyait notamment la levée des délais prévus contractuellement, de sorte qu'un client pouvait bénéficier d'une période de suspension au-delà de 12 mois, sans période minimale imposée, ni délai à respecter entre deux demandes de suspension.

Cela étant, la Banque avait répondu à Madame et Monsieur X que leur première demande n'entrait pas dans le système dérogatoire, dans la mesure où elle remplissait les conditions contractuelles. Pourtant, Madame et Monsieur X avaient insisté auprès de leur conseiller pour qu'il confirme que leur demande entrait dans le système dérogatoire, ce qu'il avait fait. C'est à ce titre qu'ils engageaient la responsabilité de la Banque.

Les conclusions de la Médiatrice

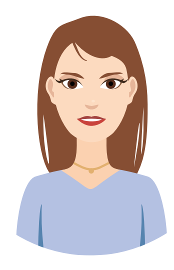
En conséquence, le système dérogatoire n'ayant pas vocation à s'inscrire dans la durée, il m'apparaît que la Banque n'a pas engagé sa responsabilité en refusant, de mettre en place un second report de mensualités, sollicité par Madame et Monsieur X, dans la mesure où les dispositions contractuelles n'étaient pas remplies, à savoir un délai minimum à respecter entre deux demandes de suspension.

Néanmoins, j'estime que la réponse apportée par le conseiller était confuse, privant les clients de la possibilité de prendre une décision parfaitement éclairée sur les modalités de la suspension de leur prêt.

En conclusion, je considère qu'en droit la Banque n'engage pas sa responsabilité en refusant de mettre en place un second report de mensualités de prêt sollicité avant l'échéance du délai d'attente prévu contractuellement.

En équité, toutefois, j'ai préconisé que la Banque leur accorde un soutien financier sous la forme d'un geste, au titre de l'absence de clarté de sa réponse alors qu'elle revêtait un caractère majeur dans leur prise de décision. ◆

Fonctionnement d'un prêt lissé



Florence

Les faits

Au moment de l'achat de leur résidence principale, Monsieur et Madame X ont eu recours pour leur financement immobilier à un prêt lissé : le 1er prêt (Prêt A) sur une durée de 120 mois avec une mensualité importante ; et le 2e prêt (Prêt B) d'une durée de 220 mois ayant une mensualité moins importante. Par le mécanisme du lissage, au terme du Prêt A, soit à la 121e mois, débute la hausse de la mensualité du Prêt B.

Quelques années après Monsieur et Madame X décident de renégocier le taux d'un de leurs prêts et signent des avenants de modifications aux nouvelles conditions demandées, et acceptées par eux par deux fois.

Six ans après la mise en place des avenants, Monsieur et Madame X constatent une hausse importante due au paiement en même temps de la mensualité des deux prêts, et cela sur une période d'un an.

Ils considèrent que cette hausse va engendrer pour eux une situation financière très délicate les bloquant pour la mise en place d'un nouveau projet immobilier compte tenu de l'augmentation de leur taux d'endettement, dépassant les 33 %.

Néanmoins, la Banque insiste sur la connaissance par Monsieur et Madame X des nouvelles conditions qui sont la résultante des modifications qu'ils ont expressément sollicitées et dont ils ont été informés.

Monsieur et Madame X m'ont saisie considérant que l'établissement bancaire aurait commis une erreur sur le lissage des deux prêts immobiliers. Ils souhaitent obtenir le remboursement de la somme de 9573€ payée pendant cette période de hausse.

L'analyse de la Médiatrice

J'ai constaté que Monsieur et Madame X ont opté pour un prêt lissé lors de la souscription de leurs prêts immobiliers, leur permettant d'harmoniser les remboursements de leurs crédits.

En effet, le principe du prêt lissé ou prêt à palier est de permettre à l'emprunteur de contracter un emprunt immobilier tout en poursuivant le remboursement de crédits préalables, en préservant un taux d'endettement égal tout au long de la période d'amortissement.

Animés par cette volonté, Monsieur et Madame X expliquent que s'ils avaient eu connaissance de cette hausse de leurs mensualités, ils auraient refusé de signer les avenants.Toutefois, ils ont régulièrement signé les avenants, sur lesquels ils pouvaient vérifier les caractéristiques et modalités de remboursement de leurs prêts, sans avoir, en amont, émis de réclamation sur ce sujet.

J'ai rappelé qu'en vertu de l'article 1103 du Code civil «*les contrats légalement formés tiennent lieu de loi à ceux qui les ont faits*». Il faut comprendre cette disposition comme posant la règle fondamentale selon laquelle, dès lors que le contrat est valablement conclu, il est créateur de normes pour les parties, il devient donc obligatoire.

Par conséquent, la mise en application des conditions demandées par les emprunteurs ne saurait être à l'origine de l'existence d'un dommage opposable à l'établissement de crédit. Monsieur et Madame X avaient tous les éléments pour vérifier, apprécier et prévoir cette situation momentanée dont l'existence n'est que le fruit des modifications souhaitées par eux.

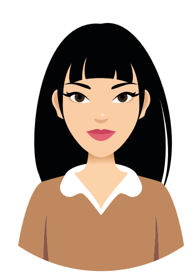
Ils avaient, à leur disposition, les tableaux d'amortissements permettant d'avoir une idée claire et précise de l'état et des modalités de remboursement faisant apparaître la coexistence des deux prêts et une hausse de la mensualité sur une période de 12 mois.

Au terme de mon analyse, il m'apparaît que Monsieur et Madame X n'ont pas été assez vigilants au moment de la signature des avenants. Ils disposaient de tous les éléments pour constater l'absence de synchronisation entre la fin du Prêt A et le début de la hausse de la mensualité du Prêt B.

La conclusion de la Médiatrice

La Banque a respecté ses obligations contractuelles dans la mise en place des avenants de renégociation et n'engage pas sa responsabilité dans leur mise en place, dès lors que les conditions et modalités sont celles souhaitées par écrit et validées par les emprunteurs à deux reprises. La Banque n'a donc aucune obligation de procéder au remboursement de la somme demandée par Monsieur et Madame X. ◆

LEP : capitalisation des intérêts et montant maximum de versement



Mélanie

Les faits

Monsieur X conteste le montant de versement maximum sur son LEP. Il souhaitait y verser en janvier 2022 la somme de 7690€ mais la banque lui a opposé un refus au motif que des intérêts du montant de 12,89€ avaient d'ores et déjà été versés sur son LEP, s'ajoutant au solde de 10€, de sorte que le plafond de

7 700 € était atteint. Monsieur X estime que le montant maximum des versements de son LEP doit être calculé sans intégrer les intérêts de l'année N-1.

L'analyse de la Médiatrice

Le LEP est un placement réglementé, réservé aux personnes domiciliées fiscalement en France à revenus modestes, proposant un taux d'intérêt garanti et exonéré d'impôt sur le revenu et de prélèvements sociaux. Ses conditions d'ouverture, son fonctionnement, sa durée et sa clôture sont définies aux articles L221-13 et suivants et R221-33 et suivants du Code monétaire et financier (CMF).

Aux termes de l'article R.221-50 du CMF le LEP est rémunéré « *selon un intérêt fixé par le Ministère de l'économie* ». L'article R.221-50 du CMF précise que les intérêts sont capitalisés « *au 31 décembre de chaque année* ». Le plafond des sommes qui peuvent être déposés sur un LEP est de 7 700 € suivant l'article D.221-46 du CMF. La capitalisation annuelle des intérêts peut dépasser ce plafond selon l'article R.221-51 du CMF « *La capitalisation prévue à l'article R.221-50 peut porter le montant du compte au-delà du plafond des dépôts autorisés mentionné à l'article D.221-46* ».

Les conclusions de la Médiatrice

Dès l'année d'ouverture, les versements sont admis, dans la limite du montant maximum autorisé de 7 700 € sauf à ce que ce plafond soit dépassé, les années suivantes, par la capitalisation des intérêts.

En juillet 2021 Monsieur X a déposé sur son LEP, la somme de 7 700 € en plusieurs fois. En octobre 2021, il a effectué un retrait de 7 690 € portant le solde de son LEP à 10 €. En décembre 2021, la banque a versé sur son LEP 12,89 € au titre des intérêts acquis sur 2021. Cette somme est automatiquement devenue du capital au 1er janvier 2022 et en conséquence, le montant cumulé du LEP atteignait 22,89 € en capital à cette date (solde 10 € + intérêts capitalisés). J'observe que c'est ce qui différencie le fonctionnement des livrets de celui du plan d'épargne logement, dans lequel le plafond des versements est calculé hors intérêts acquis, même si ces intérêts sont ensuite capitalisés.

Cela s'explique par le fait que les fonds des livrets sont en permanence disponibles et que les retraits et versements peuvent être faits à tout moment.

En conséquence je considère que Monsieur ZARIFI ne pouvait verser que la somme de 7 700 € moins celle de 22,89 €, soit **7 677,11 €**. ◆

▸ Découverte d'un ancien livret A sur support papier



Stanislas

Les faits

En vidant la maison de ses parents, Madame X a trouvé un livret d'épargne, ouvert à son nom en 1959. Madame X me saisit afin d'obtenir de la banque le versement du solde du livret ou la preuve de son transfert à la Caisse des Dépôts et Consignations.

La banque indique n'avoir trouvé en ses livres aucun compte au nom de Madame X.

L'analyse de la Médiatrice

Je rappelle que depuis la fin des années 1990, les livrets d'épargne ont été dématérialisés et remplacés par des relevés de compte périodiques. Dès lors, le livret papier de Madame X permet seulement d'attester qu'en 1959 elle détenait un livret à son nom et que son solde était de 500 francs, ce qui ne peut être retenu comme preuve de son existence en 2022.

Je rappelle ensuite qu'en matière d'archives, les pièces comptables doivent être conservées par les banques pendant une durée comprise entre 5 et 10 ans.

J'ajoute que la loi Eckert prévoit une procédure de recensement des comptes inactifs et impose aux établissements bancaires de clôturer ces comptes après 10 ans d'inactivité et d'en transférer le solde auprès de la Caisse des Dépôts et Consignations. Cette loi impose également une obligation d'information des clients, leur permettant de se manifester afin d'éviter que les fonds soient acquis à l'État à l'issue d'une période de 30 ans.

Toutefois, ces dispositions sont entrées en vigueur le 1er janvier 2016, il est donc intéressant d'observer les dispositions antérieures.

La loi du 3 janvier 1977 prévoyait à cet égard que les établissements dépositaires de fonds et de valeurs étaient autorisés à clôturer les comptes et à en transférer les avoirs auprès de la Caisse des Dépôts et Consignations lorsque qu'ils n'avaient fait l'objet d'aucune opération depuis dix années.

Un décret-loi du 30 octobre 1935 prévoyait qu'à l'issue d'un délai de 30 ans, les sommes versées à la Caisse des Dépôts et Consignations étaient acquises à l'État.

Les conclusions de la Médiatrice

En l'espèce, j'ai constaté que la dernière opération inscrite sur le livret datait de 1958. Dès lors, ce compte a pu être considéré comme inactif au plus tôt en 1989, date à laquelle les fonds inscrits sur ce livret ont pu devenir la propriété de l'État.

Par ailleurs, l'article L.123-22 du Code de commerce impose aux banques de conserver les relevés de compte pendant 10 ans. Ainsi, il ne peut être reproché à la banque de ne pas avoir retrouvé trace de ce livret, qui peut avoir été clôturé bien avant 2012.

Dans ce contexte, il ne m'a pas été possible de proposer une solution dans ce litige. ◆

Secret bancaire et accès au compte du défunt



Charlotte

Les faits

Madame X me sollicite pour obtenir de la Banque de son père défunt, la communication du solde des comptes ouverts en son nom et arrêtés au jour de son décès.

Madame X est l'une des héritières de son père avec sa dernière épouse désignée légataire universelle au-delà de la réserve héréditaire. Pourtant, elle n'a pas été convoquée à la liquidation de la succession par le notaire étranger mandaté à cet effet, **et les comptes détenus dans les livres de la Banque n'ont pas été mentionnés.** C'est la raison pour laquelle elle souhaite que la Banque lui communique des informations sur lesdits comptes, car ils sont normalement des actifs de la succession.

De son côté, la Banque explique qu'elle n'est pas en mesure de lui communiquer les informations demandées car le défunt ne disposait pas de comptes individuels **mais uniquement des comptes joints avec son épouse** et qu'en conséquence seule cette dernière était habilitée à lui délivrer des informations, **conformément au secret bancaire.**

L'analyse de la Médiatrice

J'ai relevé que la jurisprudence et la doctrine se sont prononcées sur la question et considèrent que les héritiers et les légataires universels, qui justifient de leur qualité d'ayant droit,

ne peuvent se voir opposer le secret bancaire dans la mesure où **ils continuent la personne du défunt.**

Ainsi, ils ont accès aux mêmes renseignements que ceux que le titulaire décédé du compte pouvait obtenir de son établissement bancaire.

J'ai soulevé d'ailleurs que conditionner la délivrance d'informations à l'accord du cotitulaire du compte joint serait problématique dans un contexte de conflit successoral, tel que l'expose Madame X, car il se pourrait qu'elle ne puisse jamais les obtenir, sauf à aller en justice.

J'ai également rappelé que les fonds positionnés sur un compte joint sont des avoirs communs et que le décès de l'un d'entre eux n'a pas pour effet d'éteindre ses droits et de les attribuer en totalité au seul cotitulaire survivant.

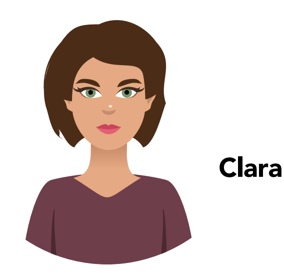
J'ai enfin soulevé que conformément à l'article 757-2 du Code civil, ce n'est qu'en l'absence d'ascendants et de descendants qu'un conjoint survivant peut recueillir toute la succession conformément à la réserve héréditaire, c'est-à-dire la part des biens et droits successoraux dont la Loi leur assure la dévolution. Ainsi, la descendante du défunt, en sa qualité d'héritière réservataire a forcément des droits sur ces fonds.

Les conclusions de la Médiatrice

Dans ces conditions j'ai considéré qu'en droit la Banque ne peut opposer à Madame X le secret bancaire pour refuser de lui communiquer le montant du solde existant au jour du décès de son père sur l'ensemble des comptes qui étaient ouverts en ses livres, et ce inclus les comptes joints.

J'ai également considéré que la Banque a manqué à ses obligations en opposant le secret bancaire à Madame X et j'ai proposé à ce titre une indemnisation à hauteur de 200€. ◆

Délai de conservation des justificatifs de vente de pièce d'or par la banque



Clara

Les faits

Madame X, héritière de Monsieur X, souhaitait obtenir un justificatif de vente de pièces de Louis d'or intervenue au début des années 1980 afin de pouvoir déterminer la fiscalité applicable. Plus précisément, elle désirait connaître le nom des pièces, le poids de l'or, l'effigie et le prix réglé à l'achat.

La Banque informa Madame X se trouver dans l'impossibilité de produire le justificatif demandé au vu de l'ancienneté de l'achat.

L'analyse de la Médiatrice

Une fois rappelé le délai de conservation de dix ans, relatif aux documents comptables et aux pièces justificatives énoncé à l'article L. 123-22 du Code de commerce, je relevai que les pièces d'or avaient été acquises dans les années 1980, élément qui avait été confirmé par l'établissement bancaire. Partant, l'achat datant de plus de dix ans, la Banque n'était pas tenue de conserver les bordereaux d'achat et les documents précis sur les pièces.

Néanmoins, comprenant l'embarras de Madame X, je l'invitai à se rapprocher de l'entité à laquelle elle souhaite vendre les pièces afin qu'elles soient évaluées ou alors d'un commissaire-priseur.

Concernant la fiscalité liée à la vente de pièces d'or, je lui conseillai de se rapprocher de l'Administration fiscale tout en lui précisant qu'un régime fiscal particulier était applicable aux ventes de pièces d'or émises antérieurement à 1800, ce qui est le cas des Louis d'or.

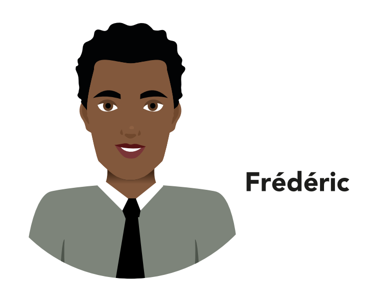
En effet, il est possible d'opter pour la taxe forfaitaire sur les métaux précieux ou pour la taxe sur les plus-values.

- la taxe forfaitaire sur les objets précieux notamment si les pièces d'or sont assimilées à des objets de collection, ce qui est souvent le cas concernant les pièces frappées avant 1800 ;
- la taxe sur les plus-values qui se calcule avec la différence entre le prix de vente et le prix d'achat. Si celle-ci est nulle ou négative la particulier n'est alors pas imposé. En revanche, si elle est positive, le taux global d'imposition de la plus-value est de 36,2 % (17,2 % de prélèvements sociaux et 19 % d'impôt). Il convient de préciser que dans ce régime il y a un abattement de 5 % par année de détention et une exonération totale d'impôt après 22 ans, d'où l'intérêt de conserver tous les justificatifs d'achat. Effectivement, ce régime s'applique seulement si le vendeur peut justifier de la date et du prix de l'acquisition des pièces, que le vendeur et l'acheteur sont la même personne (hors succession) et que les pièces à vendre sont bien les mêmes que celles achetées.

La conclusion de la Médiatrice

En l'espèce, je ne pus que constater que la vente des pièces d'or datait de plus de dix ans et que la Banque n'était donc pas tenue de fournir des justificatifs conformément au délai de conservation prévu par le Code de commerce. ◆

Obtention d'une pièce comptable couverte par le secret professionnel. Incidence en terme d'archivage



Frédéric

Les faits

Monsieur X cherchait à obtenir le justificatif complet d'une opération bancaire qu'un l'établissement bancaire ne pouvait lui communiquer au regard du secret bancaire.

Mécontent de cette décision Monsieur X décidait de faire appel à la Médiation.

L'analyse de la Médiatrice

Ce secret ne peut être opposé à l'Autorité judiciaire agissant dans le cadre d'une procédure pénale.

J'ai donc considéré que Monsieur X pouvait solliciter judiciairement la communication qu'il souhaitait en demandant à la Police (auprès de laquelle il lui appartenait de porter plainte) d'agir par la voie d'une réquisition judicaire.

La conclusion de la Médiatrice

À titre de solution au différend entre les parties j'ai validé l'obtention d'une réquisition judiciaire comme étant propre à légitimer vis-à-vis de l'établissement bancaire la communication que Monsieur X demandait.

Alors que la pièce réclamée était une pièce comptable à conserver en vertu de l'article L 123-22 du Code de commerce pendant 10 ans, j'ai en outre prescrit, cette limite de détention étant en passe d'être atteinte, que l' établissement bancaire prenne toute disposition pour conserver pendant un délai supplémentaire raisonnable, la pièce objet du litige avec Monsieur X. ◆

Annexes

CES INFORMATIONS SONT DISPONIBLES SUR NOTRE SITE INTERNET ET PLUS ENCORE



www.lemediateur.fbf.fr

- Biographie de la Médiatrice
- Charte de la médiation auprès de la FBF pour les particuliers
- Qu'est-ce que la médiation de la consommation ?

INFORMATIONS PRATIQUES POUR SAISIR LA MÉDIATRICE



Conditions pour saisir la médiatrice

La Médiatrice ne peut être saisie que :

1. par un client d'une banque adhérente au service de médiation (cf. Liste des banques adhérentes en 2022, page 44);
2. après avoir fait une demande écrite auprès de son établissement bancaire;
si la réponse apportée n'est pas satisfaisante ou en cas d'absence de réponse dans les deux mois, la Médiatrice peut être saisie.
3. si la réclamation est datée de moins d'un an;
4. si le consommateur est une personne physique, n'agissant pas pour des besoins professionnels;
5. si le litige n'est pas ou n'a pas été examiné par un autre médiateur ou par un tribunal.

Comment saisir la Médiatrice

Pour une saisine par courrier postal :

Madame la Médiatrice auprès de la FBF
CS 151
75422 PARIS Cedex 9

Les informations utiles et nécessaires à l'étude du dossier sont les suivantes :

- le nom du demandeur ainsi que ses coordonnées postales complètes et lisibles, éventuellement une adresse mail et/ou un numéro de téléphone;
- le nom complet de l'établissement bancaire et son adresse (pour les mutualistes, préciser la caisse);
- la description claire de l'objet du litige et de la demande;
- la **copie** de tous les échanges de courriers, courriels, copies d'écran (si des messages ont été envoyés depuis une plateforme Internet), et les copies des contrats et relevés de compte nécessaires à la compréhension du litige.

Ne pas agrafer, ni coller, ni scotcher les pièces jointes. Il est préférable d'éviter d'envoyer des documents originaux.

Pour une saisine en ligne :

Sur le site : https://lemediateur.fbf.fr/ (cliquer sur «saisir la médiatrice»), remplir le formulaire et joindre les échanges de courriers, courriels, copies d'écran et les copies des contrats et relevés de compte nécessaires à la compréhension du litige.

L'ajout des pièces annexes est très important pour la bonne compréhension de la demande de médiation.

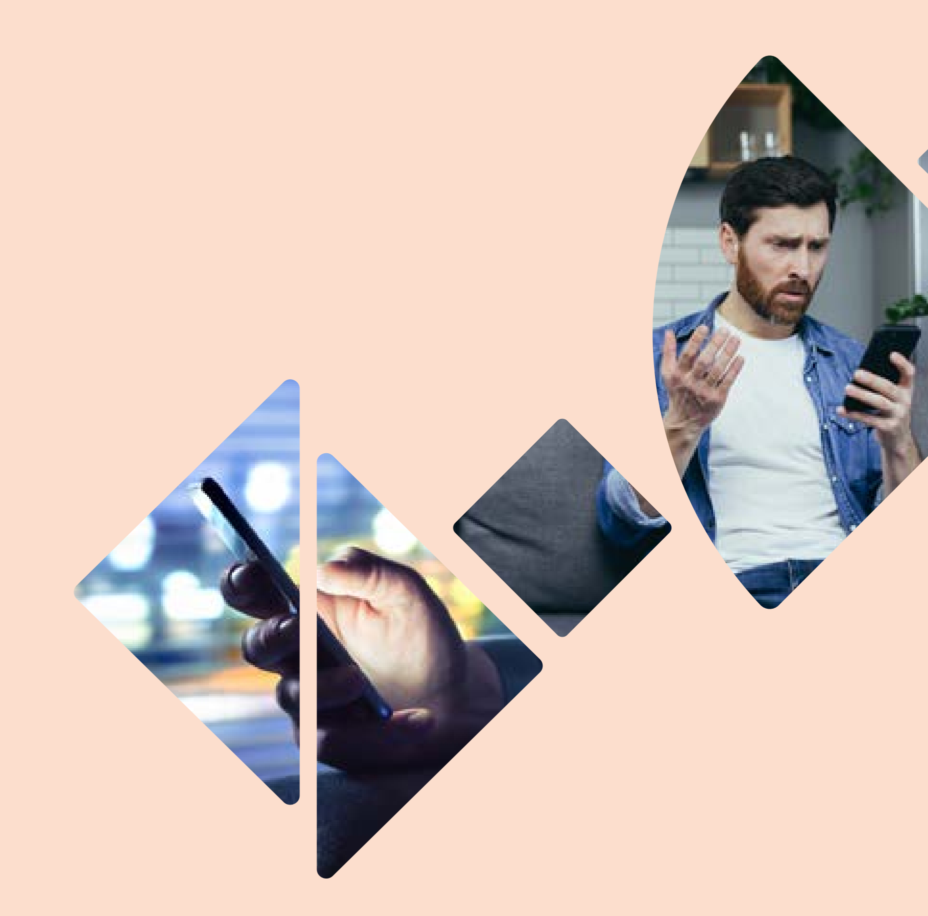
LISTE DES BANQUES ADHÉRENTES 2022



41829	Al Khaliji France SA
12240	Allianz Banque
23890	Attijariwafa Bank Europe
12548	Axa Banque
41189	Banco Bilbao Vizcaya Argentaria
19229	Banco Sabadell
41139	Banco do Brasil
44729	Banco Santander SA
18089	Bank Audi France
41259	Bank Melli Iran
18769	Bank of China Paris Branch
14879	Bank of India
44269	Bank Saderat Iran
17579	Bank Tejarat
12179	Banque Intercontinentale Arabe - BIA
17499	Banque Calédonienne d'Investissement - BCI
12468	Banque Cantonale de Genève (France) SA
24659	Banque Chabrières
17619	Banque de l'Europe Méridionale - BEMO
44149	Banque d'Escompte (Banque Wormser Frères)
13149	Banque Edel SNC
18869	Banque Française Mutualiste - BFM
11438	Banque Hottinguer
17959	Banque Michel Inchauspe - BAMI
18569	Banque MISR
40978	Banque Palatine
17679	Banque Populaire SBE
11989	Banque Pouyanne
13579	Banque Saint Olive
17779	Banque SBA
17469	Banque Socredo
16218	Bforbank
17599	Banque Banorient France (ex Blom Bank France)
12249	BMCE Bank International PLC
40618	Boursorama Banque
23779	Byblos Bank Europe SA
13335	Caisse d'Épargne Aquitaine-Poitou-Charentes
18715	Caisse d'Épargne Auvergne et Limousin
14445	Caisse d'Épargne Bretagne Pays-de-Loire
12135	Caisse d'Épargne Bourgogne Franche-Comté
14505	Caisse d'Épargne Loire-Centre
13135	Caisse d'Épargne Midi-Pyrénées
11425	Caisse d'Épargne Normandie
16275	Caisse d'Épargne Hauts-de-France
13825	Caisse d'Épargne Rhône-Alpes
12619	Caixa Geral de Depositos
41439	Banque Chaabi du Maroc
15380	Conservateur Finance
17206	Crédit Agricole Alsace Vosges
14706	Crédit Agricole Atlantique-Vendée
18706	Crédit Agricole Brie-Picardie
14806	Crédit Agricole Centre-Loire
19506	Crédit Agricole Centre-Ouest
11706	Crédit Agricole Charente Maritime Deux-Sèvres
31489	Crédit Agricole Corporate and Investment Bank (CACIB)
12506	Crédit Agricole Franche-Comté
14006	Crédit Agricole Guadeloupe
19906	Crédit Agricole Réunion
17906	Crédit Agricole Anjou-Maine
12206	Crédit Agricole Côtes-d'Armor
12906	Crédit Agricole Finistère
13606	Crédit Agricole Ille et Vilaine
43799	Crédit Agricole Indosuez Wealth Management
19806	Crédit Agricole Martinique Guyane
16006	Crédit Agricole Morbihan
16706	Crédit Agricole Nord de France
11206	Crédit Agricole Nord Midi-Pyrénées
18306	Crédit Agricole Normandie-Seine
16906	Crédit Agricole Pyrénées-Gascogne
13906	Crédit Agricole Sud Rhône-Alpes
13106	Crédit Agricole Toulouse 31
19406	Crédit Agricole Touraine-Poitou
14406	Crédit Agricole Val de France
18950	Crédit Municipal d'Avignon

14078 Crédit Municipal de Lille
17620 Crédit Municipal De Nîmes
18450 Crédit Municipal de Roubaix
18169 Crédit Suisse Luxembourg Succursale France
42529 Edmond de Rothschild France
13698 Ester Finance Titrisation
17979 Europe Arab Bank SA
18689 Fransabank France SA
14120 Gresham Banque
11833 Industrial and Commercial Bank of China (ICBC) Paris Branch
30438 ING Bank N.V
30628 JP Morgan Chase Bank, N.A.
14989 KEB Hana Bank
30748 Lazard Frères Banque
18789 Mega International Commercial Bank Co.LTD.
15628 Micos Crédit Immobilier Chebanca
24599 Milleis Banque (ex Barclays Bank)
16989 Mobilis Banque
30478 Monte Paschi Banque SA
41249 MUFG Bank Ltd. (ex Bank of Tokyo-Mitsubishi Ufj)
41639 National Bank of Kuwait France SA
30007 Natixis SA
15930 Natixis Payment Solutions
18919 Natixis Wealth Management (ex Banque Privée 1818)
30788 Neuflize OBC
45850 Oddo BHF SCA
18370 Orange Bank (ex Groupama Banque)
15068 Pictet & Cie (Europe) SA
14749 Distingo Bank marque de Banque Stellantis France (ex PSA Banque France)
17919 Qatar National Bank
43789 Quilvest Banque Privée
11188 RCI Banque
13369 Rothschild Martin Maurel
16788 Santander Consumer Banque
11238 Swisslife Banque Privée
43849 Tunisian Foreign Bank
30758 UBS (France) SA
07025677 Ufifrance Patrimoine SAS
19570 Union Financière de France Banque (UFF)
14633 Western Union International Bank
19069 Banque Richelieu France (ex Kbl Richelieu Banque Privée)
18106 Crédit Agricole Savoie
30004-1 Hello Bank!
11306 Crédit Agricole Alpes Provence
30004 BNP Paribas
18079 Banque des Caraïbes (ex Société Générale Antilles Guyane)
17106 Crédit Agricole Sud Méditerranée
12879 Banque Delubac & Cie
13188 Portzamparc Sa
41919 BNP Paribas Réunion
13088 BNP Paribas Antilles Guyane
19973 Mirabaud & Cie (Europe) SA Succursale France
17939 BNP Paribas Nouvelle Calédonie
11408 Banque de Wallis & Futuna
13506 Crédit Agricole Languedoc
28533 Solarisbank AG
11689 Citibank Europe Plc
16106 Crédit Agricole Lorraine
11006 Crédit Agricole Champagne Bourgogne
17806 Crédit Agricole Centre-Est
18719 Banque Française Commerciale Océan Indien
12149 Banque de Polynésie
15178 Sogelease BDP
29333 Hsbc Private Bank Luxembourg SA
29333 Hsbc Private Banking France

Photos de couverture : AdobeStock
Conception graphique : Allégories Créations





www.lemediateur.fbf.fr

Madame la Médiatrice auprès
de la Fédération bancaire française

CS 151 - 75 422 Paris Cedex 09